ZXR10 2900 Series
Intelligent Ethernet Switch
User Manual

Version 2.0

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: (86) 755 26771900
Fax: (86) 755 26770801
URL: http://ensupport.zte.com.cn
E-mail: support@zte.com.cn

LEGAL INFORMATION

Copyright © 2010 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit ZTE technical support website http://ensupport.zte.com.cn to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	Feb. 28, 2010	First Release

Serial Number: sjzl20096848

Contents

About This Manual I
Safety Description 1
Safety Instructions 1
Safety Signs 1
System Overview 3
Product Overview 3
Switching Capability 4
Reliability 4
Service Characteristics 4
Security Control 5
QoS Guarantee 5
Management Modes 6
Functions 6
Technical Features and Parameters 8
Structure and Principle 11
Working Principle 11
Hardware Structure 12
ZXR10 2920 12
ZXR10 2920 Interfaces 13
ZXR10 2920 Indicators 13
ZXR10 2928 14
ZXR10 2928 Interfaces 14
ZXR10 2928 Indicators 14
ZXR10 2952 15
ZXR10 2952 Interfaces 15
ZXR10 2952 Interfaces 16
ZXR10 2936-FI 17
ZXR10 2936-FI Interfaces 17
ZXR10 2936-FI Indicators 17
Sub-boards 18
FGEI 19

FGFI 19
FGFE 20
FBFE 20
PON 21
Power Supply Module 21
Installation and Debugging 23
Installing the Equipment 23
Installing the Switch on Desktop 23
Installing the Switch onto a Cabinet 23
Installation of Cables 25
Installing Power Cables 25
Installing Configuration Cables 27
Installing Network Cables 28
Installing Fibers 29
Labels 30
Cable Lightning Protection Requirements 32
System Debugging 34
Connection Configuration 34
Power-on Procedure 38
Indicator Status 39
System Boot Procedure 39
Usage and Operation 43
Configuration Modes 43
Configuration through Console Port Connection 44
Configuration through TELNET Session 44
Configuration through SSH Connection 45
Configuration through SNMP Connection 46
Configuration through WEB Connection 46
Command Mode 47
User Mode 47
Global Configuration Mode 48
File System Configuration Mode 48
Layer 3 Configuration Mode 48
NAS Configuration Mode 49
SNMP Configuration Mode 49
Cluster Management Configuration Mode 49
Basic ACL Configuration Mode 50
Extended ACL Configuration Mode 50
Layer 2 ACL Configuration Mode 50
Hybrid ACL Configuration Mode 50

Global ACL Configuration Mode 51
Usage of Command Line 51
Online Help 51
Command Abbreviations 52
History Command 52
Functional Key 53
System Management 55
File System Management 55
File System Introduction 55
File System Operation 55
Configuration Task Overview 55
Directory Operation 56
File Operation 56
Downloading/Uploading Version by TFTP 56
Formatting FLASH 57
FTP Configuration 57
Import and Export of Configuration 59
Backup and Recovery of Files 59
Software Version Upgrade 60
Viewing the Version Information 60
Version Upgrade When the System is Normal 61
Version Upgrade When the System is Abnormal 62
Description about the Configuration File 64
Service Configuration 65
Port Configuration 65
Port Overview 65
Port Basic Configuration 66
Viewing Port Information 70
MAC Table Operations 71
MAC Table Overview 71
Basic Configuration of MAC Table 71
FDB Configuration Example 72
Port Mirroring Configuration 73
Port Mirroring Overview 73
Port Mirroring Basic Configuration 74
Port Mirroring Configuration Example 74
Single Port Loop Detection Configuration 75
Loop Detection Overview 75
Configuring Single Port Loop Detection 76
VLAN Configuration 78

VLAN Overview 78
Basic Configuration of VLAN 79
VLAN Configuration Example 80
GARP/GVRP Configuration 81
GARP/GVRP Overview 81
Configuring GARP/GVRP 82
GARP/GVRP Configuration Example 82
PVLAN Configuration 84
PVLAN Overview 84
Basic Configuration of PVLAN 84
PVLAN Configuration Example 84
QinQ Configuration 86
QinQ Overview 86
Basic Configuration of QinQ 87
QinQ Configuration Example 88
SQinQ Configuration 89
SQinQ Overview 89
Basic Configuration of SQinQ 90
SQinQ Configuration Example 90
LACP Configuration 91
LACP Overview 91
Basic Configuration of LACP 92
LACP Configuration Example 93
STP Configuration 94
STP Overview 94
Basic Configuration of STP 97
Configuration Example 99
STP Configuration Example 99
RSTP Configuration Example 100
MSTP Configuration Example 101
ZESR Configuration 102
ZESR Overview 102
ZESR Introduction 102
ZESR Related Concepts 103
Single-Ring Single-Domain ZESR 104
Multi-Ring Multi-Domain ZESR 105
ZESR Tangent Ring 108
Configuration Notice 108
Basic Configuration of ZESR 109
ZESR Configuration Example 112

ZESR Single Ring Networking Example 112
ZESR Multi-Ring Networking Example 114
ZESR Smart Link Networking Example 117
IGMP Snooping Configuration 119
IGMP Snooping Overview 119
Basic Configuration of IGMP Snooping 119
IGMP Snooping Configuration Example 123
IPTV Configuration 124
IPTV Overview 124
Basic Configuration of IPTV 124
IPTV Configuration Example 129
DHCP CLIENT Configuration 131
DHCP CLIENT Overview 131
Basic Configuration of DHCP CLIENT 131
DHCP CLIENT Configuration Example 132
DHCP Snooping/Option82 Configuration 133
DHCP Snooping/Option82 Overview 133
Basic Configuration of DHCP Snooping/Option82 134
DHCP Snooping/Option82 Configuration Example 135
VBAS Configuration 136
VBAS Conifguration Overview 136
Basic Configuration of VBAS 137
VBAS Configuration Example 138
EPON 138
EPON Overview 138
EPON Function of ZXR10 2900 139
Basic Configuration of EPON 140
EPON Service Switch Configuration 141
EPON Configuration Example 143
Upgrading PON Daughter Card 145
ACL Configuration 147
ACL Overview 147
Basic Configuration of ACL 148
ACL Configuration Example 154
QoS Configuraton 156
QoS Overview 156
Basic Configuration of QoS 157
QoS Configuration Example 165
Layer 2 Protocol Transparent Transmission Configuration 167

802.1x Transparent Transmission Overview 167
Basic Configuration of Layer 2 Protocol Transparent Transmission 167
Layer 2 Protocol Transparent Transmission Configuration Example 168
Layer 3 Configuration 169
Layer 3 Overview 169
Basic Configuration of Layer 3 170
Layer 3 Configuration Example 170
Access Service Configuration 171
Access Service Overview 171
Basic Configuration of Access Service 175
Access Service Configuration Example 180
Syslog Configuration 182
Syslog Overview 182
Basic Configuration of Syslog 182
Syslog Configuration Example 183
NTP Configuration 183
NTP Overview 183
Basic Configuration of NTP 183
NTP Configuration Example 184
OAM 185
OAM Overview 185
OAM Overview 185
OAM Function 185
Basic Configuration of OAM 186
OAM Configuration Example 189
OAM Remote Loopback Configuration Example 189
OAM Link Control Event Configuration Example 191
Network Management 193
Remote-Access 193
Remote-Access Overview 193
Basic Configuration of Remote-Access 193
Remote-Access Configuration Example 194
SSH 195
SSH Overview 195
Basic Configuration of SSH 195
SSH Configuration Example 196

SNMP 198
SNMP Overview 198
Basic Configuration of SNMP 199
SNMP Configuration Example 200
RMON 202
RMON Overview 202
Basic Configuration of RMON 202
RMON Configuration Example 203
Cluster Management 205
Cluster Management Overview 205
Configuring ZDP 207
Configuring ZTP 208
Configuring Cluster 209
Cluster Management Configuration Example 211
SFLOW 213
SFLOW Overview 213
Basic Configuration of SFLOW 213
WEB 214
WEB Overview 214
Configuring System Login 214
Configuration Management 216
System Information 216
Port Management 217
VLAN Management 221
PLAN Management 224
Port Mirroring Management 226
LACP Management 229
Monitor Information 233
Terminal Log 233
Port Statistics 233
Configuration Information 234
System Maintenance 235
Saving Configuration 235
Configuring Reboot 236
Uploading File 237
User Management 239
Adding User 240
Deleting User 240
Figures 243
Tables 247

Glossary 249

About This Manual

Purpose

This manual introduces structure and principles, service data configuration, network management configuration and system management.

Intended Audience

This manual is intended for the following engineers:

- On-site maintenance engineers
- Network monitor engineers
- System maintenance engineer

What Is in This Manual

ZXR10 2900 (V2.0) Series Intelligent Access Ethernet Switch User Manual contains the following chapters:

Chapter	Summary
Chapter 1 Safety Description	Describes the safety instructions and signs.
Chapter 2 System Overview	Introduces the ZXR10 2920/2928/2952/2936-FI briefly.
Chapter 3 Structure and Principles	Introduces the structure and working principles of the ZXR10 2920/2928/2952/2936-FI.
Chapter 4 Installation and Debugging	Introduces the installation and debugging methods of the ZXR10 2920/2928/2952/2936-FI.
Chapter 5 Usage and Operations	Introduces the configuration methods, command mode, and usage of command line.
Chapter 6 System Management	Introduces the system management of the ZXR10 2920/2928/2952/2936-FI.
Chapter 7 Service Configuration	Introduces the service data configuration of ZXR10 2920/2928/2952/2936-FI.
Chapter 8 Network Management	Introduces the network management configuration of the ZXR10 2920/2928/2952/2936-FI.

Related Documentation

- ZXR10 2900 (V2.0) Series Intelligent Ethernet Switch Command Reference

This page is intentionally blank.

Chapter 1

Safety Description

Table of Contents

Safety Instructions 1
Safety Signs 1

Safety Instructions

Only duly trained and qualified personnel can install, operate and maintain the devices.

During the device installation, operation and maintenance, please abide the local safety specifications and related operation instructions, otherwise physical injury may occur or devices may be broken. The safety precautions mentioned in this manual are only supplement of local safety specifications.

The **debug** commands on the devices will affect the performance of the devices, which may bring serious consequences. So take care to use **debug** commands. Especially, the **debug all** command will open all **debug** processes, so this command must not be used on the devices with services. It is not recommended to use the **debug** commands when the user networks are in normal state.

ZTE Corporation will assume no responsibility for consequences resulting from violation of general specifications for safety operations or of safety rules for design, production and use of the devices.

Safety Signs

The contents that users should pay attention to when they install, operate and maintain devices are explained in the following formats:

Warning:

Indicates the matters needing close attention. If this is ignored, serious injury accidents may happen or devices may be damaged.

Caution:

Indicates the matters needing attention during configuration.

Note:

Indicates the description, hint, tip and so on for configuration operations.

Chapter 2

System Overview

Table of Contents

Product Overview 3
Functions 6
Technical Features and Parameters 8

Product Overview

ZXR10 2920/2928/2952/2936-FI Gigabit uplink smart access switch is the important part of ZXR10 series Ethernet switch. This series product is 100Mbps L2+ (Layer2+, between layer 2 and layer 3) Ethernet switch, providing gigabit uplink Ethernet ports. It can provide different quantity and interface-types of Ethernet port, mainly located at 100Mbps access and converge, which provides fast, efficient and highly cost-effective access and convergence solutions. It is mainly applied in access layer of carrier network and enterprise network.

Port and insert-card expanding instance that ZXR10 2920/2928/2952/2936-FI switch series support are shown below.

Switch Type	Fixed Port	Expanding Module
ZXR10 2920	16 10/100 Base-T Ethernet Ports 2 10/100/1000 BASE-T Ethernet Ports	An expanding insert card which can provide dual-channel 1000M optical port , dual-channel 1000M electrical port, a 1000M electrical port together with a 1000M optical port or dual-channel 100M optical port.
ZXR10 2928	24 10/100 Base-T Ethernet Ports 2 10/100/1000BASE-T Ethernet Ports	An expanding insert card which can provide dual-channel 1000M optical port , dual-channel 1000M electrical port, a 1000M electrical port together with a 1000M optical port or dual-channel 100M optical port.

Switch Type	Fixed Port	Expanding Module
ZXR10 2952	48 10/100 Base-T Ethernet Ports 2 10/100/1000BASE-T Ethernet Ports 2 1000BASE-X Ports	Non-support
ZXR10 2936-FI	8 10/100BASE-TX Ethernet Ports 24 100BASE-FX Ethernet Optical Ports 4 1000BASE-X Ports	Non-support

Switching Capability

All the ports of ZXR10 2920/2928/2952/2936-FI support the layer-2 switching at wire-speed. The data message can be forwarded at wire-speed after be filtered and processed by flow classification. Ports provide high throughput, low packet discarding rate and low time delay and jitter, which satisfy the demand of the key application.

Reliability

ZXR10 2920/2928/2952/2936-FI ensures the redundancy backup and fast switch through STP/RSTP/MSTP. These switches support the 802.3ad LACP function and it supplies load sharing and link backup. It supports ZESR Ethernet ring network mode to provide fast protection switching, which ensures the user service will not be interrupted.

Service Characteristics

All kinds of operation characteristics and control are as follows:

1. It provides flexible VLAN classification mode. It can be classified by types of port, protocol, MAC address and so on.
2. It provides VPN on layer-2 and SelectiveQinQ through QinQ which flexibly controls outer layer label and makes operation and plan convenient.
3. It provides user port location technology such as VBAS and DHCP Option82.
4. It provides L2 multicast technology including igmp-snooping and proxy function, fast-leaving characteristic and Multicast-Vlan Switching (MVS) function, which supports for opening IPTV service.

Security Control

The functions of security control are listed below.

1. User level security control is provided.
   i. IEEE 802.1x implements dynamic and port-based security, which provides the user ID authentication function.
   ii. It supports MAC/IP/VLAN/PORT combination at random, which prevents illegal user from accessing the network effectively.
   iii. Port isolation is helpful to make sure that users can not monitor or access to other users on the same switch.
   iv. DHCP monitoring prevents spiteful users deceiving the server and sending spurious address, so it can start IP source protection and create a binding table for the IP address of the user, MAC address, ports and VLAN to prevent user deceiving or using IP address of other users.
2. Equipment level security is provided.
   i. CPU security control technology can resist DoS attack from CPU.
   ii. SSH/SNMPv3 protocol supplies network management security.
   iii. Multilevel security of console can prevent unauthenticated users changing the switch configuration.
   iv. RADIUS identification authentication puts the switch under the centralized control and prevents unauthorized user from modifying configuration.
3. Network security control is provided.
   i. ACL based on port or Trunk makes it possible for users to apply security strategy to the ports of switches or Trunk.
   ii. MAC address binding and the filter based on source or destination provide effective flow control based on address.
   iii. Port mirroring function provides an effective tool for network management analysis.

QoS Guarantee

Applications of QoS are shown below:

1. Standard 802.1p CoS and DSCP field sort can be labeled and sorted again based on single packet with source and destination IP address, source and destination MAC address, and TCP/UDP port number.
2. It provides queue schedule algorithm: Strict Priority (SP) and combination schedule (SP+WRR). Of which WRR is the abbreviation of Weighted Round Robin.
3. It supports Committed Access Rate (CAR) function. It manages the asynchronous uplink and downlink data flow from end

stage or up link by utilizing input strategy and output shaping. Input strategy control supplies the bandwidth control with minimal increment of 64kbps. When network congestion occurs, it still can satisfy the QoS demands of discarding packets, time delay and time jitter. As a result, queue congestion can be avoided effectively.

Management Modes

Switch management is described with the following statements.

1. It supports SNMPv1/v2c/v3 and RMON.
2. It supports ZXNM01 uniform network management platform.
3. It supports CLI command lines including Console, Telnet and SSH to access the switch.
4. It supports Web network management.
5. It supports ZTE Group Manage Protocol (ZGMP) group management.

Functions

ZXR10 2920/2928/2952/2936-FI adopts Store and Forward mode, and supports layer-2 switching at wire-speed. Full wire-speed switching is implemented at all ports.

ZXR10 2920/2928/2952/2936-FI has the following functions:

1. 100Mbps ports support 10/100M self adaption and MDI/MDIX self adaption.
2. Gigabit electrical ports support port 10/100/1000M self adaption and MDI/MDIX self adaption.
3. It supports port–based 802.3x flow control (full duplex) and back-pressure flow control (half duplex).
4. It supports Virtual Circuit Tester (VCT) function.
5. It supports VLAN complying with 802.1q. The maximum number of VLANs can be up to 4094.
6. It supports VLAN stacks function (QINQ), and outer label is optional (SQinQ).
7. It supports GVRP dynamic VLAN.
8. It has the capability of MAC addresses self-learning. The size of the MAC address table is up to 8K.
9. It supports port MAC address binding and addresses filtering.
10. It supports the function of port security and port isolation.
11. It supports the STP defined in the 802.1d, RSTP defined in the 802.1w, and MSTP defined in the 802.1s. The maximum number of the example can be up to 16.

12. It supports ZESR technology.
13. It supports LACP port binding defined in 802.3ad and port static binding. At most 15 port groups can be bound and each group contains at most 8 ports.
14. It supports cross-VLAN IGMP snooping and MVS controllable multicast technology.
15. It supports single port loop test.
16. It supports 802.1x user authentication.
17. Port location supports VBAS and DHCP-OPTION82.
18. It supports DHCP-SNOOPING.
19. It supports broadcast storm suppression.
20. It supports port ingress and egress mirror, and flow-based mirror and statistics.
21. It supports ACL function based on port and Trunk. The ACL rule can be set according to time segment.
22. It supports IETF-DiffServ and IEEE-802.1p standard. The 100M port supports 4 priority queues. The Gigabit port supports 8 priority queues. Ingress supports CAR. The queue scheduling supports SP and combination (SP+WRR) scheduling method. It supports egress shaping and tail-drop.
23. Port-based speed control includes input speed limit and output speed limit. Input speed limit supports flow rate limit of multiple buckets, and output speed limit is based on queue. The minimal granularity is 64Kbps.
24. It provides detailed port flow statistics.
25. It supports 802.3ah Ethernet OAM.
26. It supports SFLOW.
27. It supports L2 protocol transparent transmission.
28. It supports syslog function.
29. It supports the function of NTP client end.
30. It supports network management static route configuration.
31. It supports ZGMP group manage.
32. It supports SNMPv1/v2c/v3 and RMON.
33. It supports Console configuration, Telnet remote login.
34. It supports SSHv2. 0.
35. It supports WEB function.
36. It supports ZXNM01 unified network management.
37. It supports the uploading and downloading of TFTP version.

Technical Features and Parameters

ZXR10 2920/2928/2952/2936-FI technical features and parameters are given in Table 1.

TABLE 1 TECHNICAL FEATURES AND PARAMETERS

Item	Description
Size	ZXR10 2920: 43.6 mm(High)×436 mm(Width)×200 mm(Depth) ZXR10 2928: 43.6 mm(High)×436 mm(Width)×200 mm(Depth) ZXR10 2952: 43.6 mm(High)×442 mm(Width)×280 mm(Depth) ZXR10 2936–FI: 43.6 mm(High)×426 mm(Width)×280 mm(Depth)
Weight (with the full configuration)	ZXR10 2920: 2 kg ZXR10 2928: 2 kg ZXR10 2952: 2.5 kg ZXR10 2936–FI: 4 kg
Maximum Power Consumption	ZXR10 2920: 16 W ZXR10 2928: 20 W ZXR10 2952: 27 W ZXR10 2936–FI: 40 W
Switch Capacity	ZXR10 2920: 11.2 Gbps ZXR10 2928: 12.8 Gbps ZXR10 2952: 17.6 Gbps ZXR10 2936–FI: 14.4 Gbps
Packet Forwarding Rate	ZXR10 2920: 8.3 Mpps ZXR10 2928: 9.5 Mpps ZXR10 2952: 13.1 Mpps ZXR10 2936–FI: 10.7 Mpps
Average Invalid Time	MTBF: ZXR10 2920: 592485.51 hours ZXR10 2928: 545141.7 hours ZXR10 2952: 372794.69 hours ZXR10 2936–FI: 351996.28 hours

Item	Description
Power	AC Power Supply: 100 V~240 V, 48 Hz~62 Hz, Wave shape distortion <5% DC Power Supply: -57 V~-40 V
Environment	Temperature (℃): For long-term work[1] 15 ℃~30 ℃ For short-term work[2] -5 ℃~45 ℃ Relative Humidity (%): For long-term work 30%~70% For short-term work 20%~90%

1. Under the normal work environment, the test point of temperature and humidity should be above ground 2 meters and anterior to equipment 0.4m (when the equipment without front and back protection board.)
2. The short-term work means the continuous operation is less than 48 hours, and the annual work time is accomplished within 15 days.

This page is intentionally blank.

Chapter 3

Structure and Principle

Table of Contents

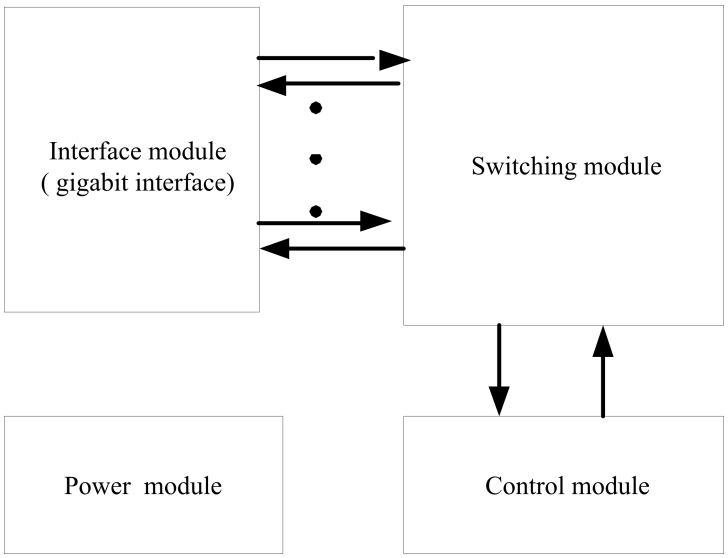
Working Principle.....11
Hardware Structure 12
Sub-boards.....18
Power Supply Module 21

Working Principle

ZXR10 2920/2928/2952/2936-FI series products have powerful functions and sound performance. According to system functions, the product contains the following modules: control module, switching module, interface module and power module. System principle figure is shown as Figure 1.

1. Control Module: Control module consists of main processor and external functional chips to implement applications such as switching module control and manage for the system. It provides serial ports for data operation and maintenance.
2. Switch Module: The main part of switch module is dedicated Ethernet switch chip, which is used to process and switch packets sent from ports.
3. Interface Module: The main part of interface module is physical layer chip, mainly used for connection to external users and packet forwarding.
4. Power Module: Power module adopts the 220 V AC or -48 V DC to offer the required power supply for other parts of the system.

FIGURE 1 ZXR10 2920/2928/2952/2936-FI WORKING PRINCIPLE



Hardware Structure

ZXR10 2920/2928/2952/2936-FI adopts the box structure with 1U high. The hardware structure consists of box, power supply and Ethernet switching main board and so on.

The box is mainly composed of chassis and shell with light weight and simple structure, which is convenient for installation and disassembly. On the front panel of ZXR10 2920/2928/2952/2936-FI, there are service interfaces, serial configuration port and system status indicators. On the back panel of ZXR10 2920/2928/2952/2936-FI, there are AC and DC power supply interface and power supply switch. ZXR10 2920/2928/2952 adopts natural dissipation method, the vents on the left and right sides of box. ZXR10 2936-FI adopts active ail-cooled heat method, the exhaust fan is installed on the one side of switch.

Power supply adopts independent power supply and supports two modes for power supply: -48V DC and 110V/220V AC.

The core hardware of ZXR10 2920/2928/2952/2936-FI is the Ethernet switching main board, which implements the switching and forwarding function of switch.

ZXR10 2920

Front panel of ZXR10 2920 is shown in Figure 2.

FIGURE 2 ZXR10 2920 FRONT PANEL

ZXR10 2920 Interfaces

ZXR10 2920 provides the following types of access ports.

1. 16 fixed 10/100 BASE-T Ethernet ports, which support full/half duplex, 10/100M adaptation, MDI/MDIX adaptation and VCT automatic test function.
2. Two fixed 10/100/1000 BASE-T Ethernet ports.
3. One expansion slot (two 1000M optical ports , two 1000M electrical ports, one 1000M electrical port together with one 1000M optical port, or two 100M optical ports can be expanded).
4. One console port is to realize the management and configuration of various services.

ZXR10 2920 Indicators

The following indicators are adopted on the front panel of ZXR10 2920.

- 32 indicators indicate the status of the 16 10/100Base-T ports. Each port has two indicators. The left indicator of port indicates the status of half/full duplex. The right indicator of port indicates the status of LINK/ACT.
- Four indicators show the status of two 10/100/1000 BASE-T ports. Each port has two indicators. The left indicator of port shows the status of ACT. The right indicator of port shows the status of LINK.
- Two system indicators show the system running work status.

Indicators running statuses are described as follows:

1. System indicators include power indicator (SYS) and running indicator (RUN).
   - After the system is powered up, the SYS indicator is on and the RUN indicator is off.
   - When BootROM starts to load the version, if the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at a frequency of one time per second.
2. The indicators of ZXR10 2920 (except power and system indicators) are shown in Table 2.

TABLE 2 INDICATOR WORKING STATE OF ZXR10 2920

Indicator	Position	State	Meaning
10/100 Base-T Ports	On the left side of port	On	Full-duplex
		Off	Half-duplex
		Flashing	Collision condition
	On the right side of port	On	Link is available.

Indicator	Position	State	Meaning
		Flashing	Data is sent and received.
10/100/1000 BASE-T Ports	On the left side of port	ACT indicator is flashing.	Data is sent and received.
	On the right side of port	LINK indicator is always on.	LINK is available.

ZXR10 2928

Front panel of ZXR10 2928 is shown in Figure 3.

FIGURE 3 FRONT PANEL OF ZXR10 2928

ZXR10 2928 Interfaces

ZXR10 2928 provides the following types of access ports.

1. 24 fixed 10/100 BASE-T Ethernet ports, which support full/half duplex, 10/100M adaptation , MDI/MDIX adaptation and VCT automatic test function.
2. Two fixed 10/100/1000 BASE-T Ethernet ports.
3. One expansion slot (two 1000M optical ports , two 1000M electrical ports, one 1000M electrical port together with one 1000M optical port, or two 100M optical ports can be expanded).
4. One console port is to realize the management and configuration of various services.

ZXR10 2928 Indicators

The following indicators are adopted on the front panel of ZXR10 2928.

- 48 indicators indicate the statuses of the 16 10/100 Base-T ports. Each port has two indicators. The left indicator of port indicates the status of half/full duplex. The right indicator of port indicates the status of LINK/ACT.
- Four indicators show the statuses of two 10/100/1000 BASE-T ports. Each port has two indicators. The left indicator of port shows the status of ACT. The right indicator of port shows the status of LINK.
- Two system indicators show the system running work status.

Indicator running statuses are described as follows:

1. System indicators include power indicator (SYS) and running indicator (RUN).
   - After the system is powered up, the SYS indicator is on and the RUN indicator is off.
   - When BootROM starts to load the version, if the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at a frequency of one time per second.
2. The indicators of ZXR10 2928 (except power and system indicators) are shown in Table 3.

TABLE 3 INDICATOR WORKING STATE OF ZXR10 2928

Indicator	Position	State	Meaning
10/100 Base-T Ports	On the left side of port	On	Full-duplex
		Off	Half-duplex
		Flashing	Collision condition
	On the right side of port	On	Link is available.
		Flashing	Data is sent and received.
10/100/1000 BASE-T Ports	On the left side of port	ACT indicator is flashing.	Data is sent and received.
	On the right side of port	LINK indicator is always on.	LINK is available.

ZXR10 2952

Front panel of ZXR10 2952 is shown in Figure 4.

FIGURE 4 ZXR10 2952 FRONT PANEL

ZXR10 2952 Interfaces

ZXR10 2952 provides the following types of access ports.

1. 48 fixed 10/100 BASE-T Ethernet ports, which support full/half duplex, 10/100M adaptation, MDI/MDIX adaptation and VCT automatic test function.
2. Two fixed 10/100/1000 BASE-T Ethernet ports.
3. Two fixed 1000BASE-X interfaces.

4. One console port is to realize the management and configuration of various services.

ZXR10 2952 Interfaces

The following indicators are adopted on the front panel of ZXR10 2952.

- There are 48 indicators on the front panel of ZXR10 2952, indicating the LINK/ACT status of the 48 10/100 Base-T ports. There are two indicators on the top of each column. The left indicator shows the status of the lower port (odd port). The right indicator shows the status of the upper port (even port).
- Four indicators show the status of two 10/100/1000 BASE-T port. Each port has two indicators. The left indicator of port shows ACT status. The right indicator of port shows LINK status.
- Two indicators show the LINK/ACT status of two 1000BASE-X ports. The indicators on the right side of optical port, each port has an indicator. The upside indicator corresponds to the upside optical port, the downside indicator corresponds to the downside optical port.
- Two system indicators show power indicator (SYS) and running indicator (RUN).

Indicators running status are described as follows:

1. System indicators include power indicator (SYS) and running indicator (RUN).
   - After the system is powered up, the SYS indicator is on and the RUN indicator is off.
   - When BootROM starts to load the version, if the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at a frequency of one time per second.
2. The indicators of ZXR10 2952 (except power and system indicators) are shown in Table 4.

TABLE 4 INDICATOR WORKING STATE OF ZXR10 2952

Indicator	Position	State	Meaning
10/100 Base-T Ports	On the left side of port, it shows the status of the lower port (odd port)	Flashing	Ports are UP.
	On the right side of port, it shows the status of the upper port (even port)		

Indicator	Position	State	Meaning
10/100/1000 BASE-T Ports	On the left side of port	ACT indicator is flashing.	Data is sent and received.
	On the right side of port	LINK indicator is on.	LINK is available.
1000 BASE-X Ports	The indicators on the right side of optical port, each port has one indicator, the upside indicator corresponds to the upside optical port, the downside indicator corresponds to the downside optical port.	On	LINK is available.
		Flashing	Data is sent and received.

ZXR10 2936-FI

Front panel of 2936-FI is shown in Figure 5.

FIGURE 5 ZXR10 2936-FI FRONT PANEL

ZXR10 2936-FI Interfaces

ZXR10 2936-FI provides the following types of access ports.

1. Eight 10/100 BASE-TX Ethernet 100M electrical ports. These ports support MDI/MDIX adaptation function and VCT automatic test function.
2. 24 100BASE-FX Ethernet 100M optical ports.
3. Four uplink 1000BASE-X interfaces.
4. One console port is to realize the management and configuration of various services.

ZXR10 2936-FI Indicators

The following indicators are adopted on the front panel of ZXR10 2936-FI.

- 56 indicators indicate the status of the 28 optical ports. Each port has two indicators. The upside indicator shows the LINK

status of port. The downside indicator shows the ACT status of port.

- 16 indicators show the status of 8 10/100 BASE-T ports. Each port has two indicators. The left indicator of port shows ACT status. The right indicator of port shows LINK status.
- Two system indicators show power indicator (SYS) and running indicator (RUN).

Indicators running status are described as follows:

1. System indicators include power indicator (SYS) and running indicator (RUN).
   - After the system is powered up, the SYS indicator is on and the RUN indicator is off.
   - When BootROM starts to load the version, if the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at a frequency of one time per second.
2. The indicators of ZXR10 2936-FI (except power and system indicators) are shown in Table 5.

TABLE 5 INDICATOR WORKING STATE OF ZXR10 2936-FI

Indicator	Position	State	Meaning
100BASE-FX/ 1000BASE-X Ports	The upside indicator	LINK indicator is on.	LINK is available.
	The downside indicator	ACT indicator is flashing.	Data is sent and received.
10/100BA-SE-TX Ports	On the left side of port	ACT indicator is flashing.	Data is sent and received.
	On the right side of port	LINK indicator is on.	LINK is available.

Sub-boards

FGEI, FGFI, FGFE and FBFE can be chosen for ZXR10 2920/2928 according to the practical networking. The corresponding types and functions are shown in Table 6.

TABLE 6 ZXR10 2920/2928 SUB-BOARD LIST

Sub-board	Model	Function
FGEI	RS-2800-2GE-RJ45	dual-channel 1000M electrical ports
FGFI	RS-2800-2GE-SFP	dual-channel 1000M optical ports

Sub-board	Model	Function
FGFE	RS-2800-2GE-SFPRJ45	one 1000M electrical port together with one 1000M optical port
FBFE	RS-2800-2FE-SFP	dual-channel 100M optical ports

Note:

The above sub-boards do not support hot-plug. The sub-board is not the standard configuration when equipment is dispatched. Therefore, the switch with or without sub-board depends on its actual configuration.

FGEI

FGEI offers two gigabit Ethernet uplink electrical ports. The type is RS-2800-2GE-RJ45 and supports 10/100/1000M adaptive, as shown in Figure 6.

FIGURE 6 RS-2800-2GE-RJ45 SUB-BOARD(FGEI)

There are 4 indicators on the FGEI panel. Each gigabit Ethernet electrical port has 2 indicators. One is link activation indicator, the other is link status indicator.

1. When the link activation indicator is flashing, it indicates that the data is sent or received.
2. When the link status indicator is on, it indicates that the LINK status is normal.

FGFI

FGFI offers two gigabit Ethernet uplink optical ports, the type is RS-2800-2GE-SFP, as shown in Figure 7.

FIGURE 7 RS-2800-2GE-SFP SUB-BOARD(FGFI)

There are 2 indicators on the FGFI panel: ACT1 and ACT2, corresponding to the two gigabit optical ports respectively. When the indicator is on, it indicates that LINK is normal. If the indicator is flashing, it indicates that there is packet being received or sent.

FGFE

FGFE offers 1 gigabit Ethernet uplink optical port and 1 gigabit Ethernet uplink electrical port. The type is RS-2800-2GE-SFPRJ45, as shown in Figure 8.

FIGURE 8 RS-2800-2GE-SFPRJ45 SUB-BOARD(FGFE)

There are 3 indicators on the FGFE panel. The gigabit optical port has an indicator ACT. When the indicator is on, it indicates that LINK is normal. If the indicator is flashing, it indicates that there is packet being received or sent. The gigabit electrical port has two indicators: one is link activation indicator and the other is link status indicator.

1. If the link activation indicator is flashing, it indicates that there is packet being received or sent.
2. When link status indicator is on, it indicates that the LINK is normal.

FBFE

FBFE offers two 100M Ethernet uplink optical ports, and the type is RS-2800-2FE-SFP, as shown in Figure 9.

FIGURE 9 RS-2800-2FE-SFP(FBFE)

There are 2 indicators on the FBFE panel: ACT1 and ACT2, corresponding to the two 100M optical ports respectively. When the indicator is on, it indicates that LINK is normal. If the indicator is flashing, it indicates that there is packet being received or sent.

PON

PON offers a Gigabit bi-directional optical port, and the type is RS-2800-1GE-SFF, as shown in Figure 10.

FIGURE 10 RS-2800-1GE-SFF

There are an indicator ACT on the PON panel which corresponds to PON optical port. When the indicator is on, it indicates that LINK is normal. If the indicator is flashing, it indicates that there is packet being received or sent.

Note:

ZXR10 2920/2928 can act as ONU device after loading PON sub-board. After connecting the single mode bi-directional optical port to OLT side of central office end, the device accesses EPON network system.

Power Supply Module

ZXR10 2920/2928/2952/2936-FI supports two power supply modes: -48V DC power supply and 110V/220V AC power supply.

When the -48V DC power supply is adopted, use –48V DC power cable. When the AC power supply is adopted, use AC power cable. Figure 11 shows the back panel of the switch when the -48V DC power supply is used. Figure 12 shows the back panel of the switch when the 110V/220V AC power supply is used.

FIGURE 11 ZXR10 2920/2928/2952/2936-FI BACK PANEL (DC POWER)

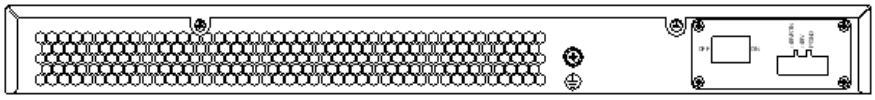
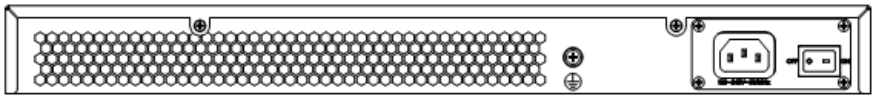


FIGURE 12 ZXR10 2920/2928/2952/2936-FI BACK PANEL (AC POWER)



Chapter 4

Installation and Debugging

Table of Contents

Installing the Equipment.....23
Installation of Cables 25
Cable Lightning Protection Requirements 32
System Debugging 34

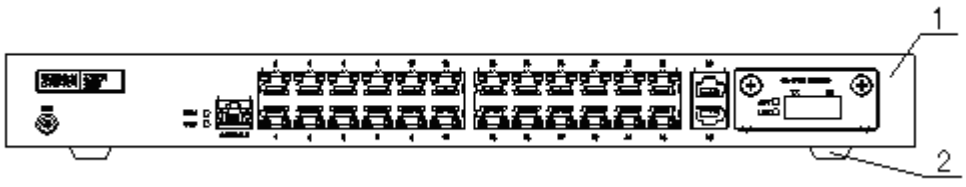
Installing the Equipment

ZXR10 2920/2928/2952/2936-FI can be installed on desk or in 19-inch standard cabinet.

Installing the Switch on Desktop

When switch is placed on desktop, install four plastic pads (the plastic pads and screws are part of the accessories) on bottom plate of switch. It is shown in Figure 13

FIGURE 13 INSTALLING PLASTIC PADS



1. Case
2. Pad

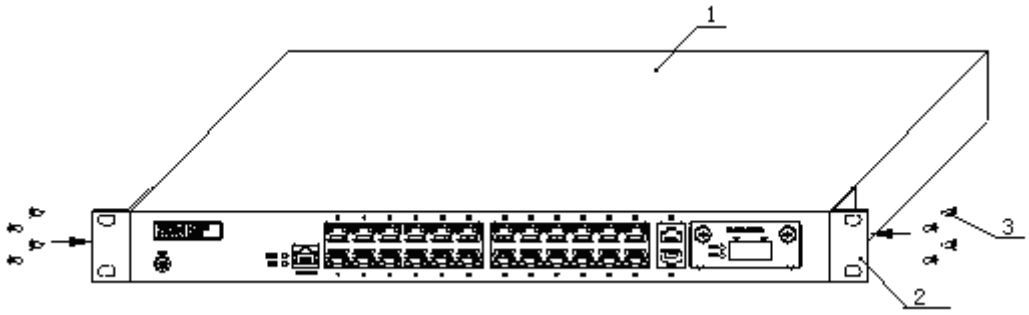
Installing the Switch onto a Cabinet

Switch can either be installed on a desktop or in 19-inch cabinet. Where, 19-inch standard cabinet can be provided by the user. In case ZTE cabinet is to be used, please refer to 19-Inch Standard

Cabinet Installation Manual for cabinet installation. To install a switch onto a cabinet, perform the following steps.

1. Fix two flanges (both flanges and screws are provided together with device) on two sides of switch shell, as shown in Figure 14.

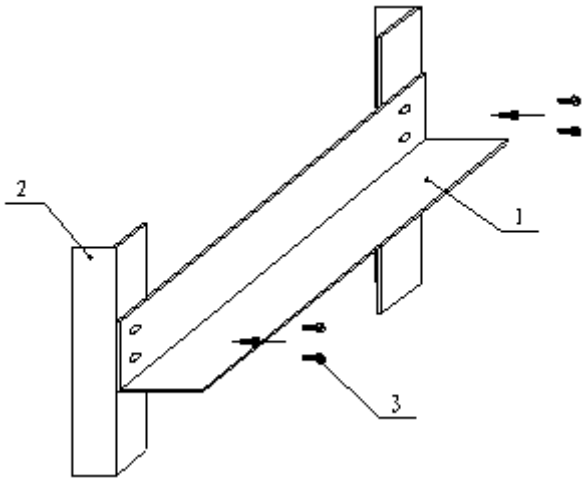
FIGURE 14 INSTALLING FLANGES



1. Case
2. Flange
3. Screw

2. Install two symmetrical brackets at both sides of the 19-inch cabinet to support the switch, as shown in Figure 15.

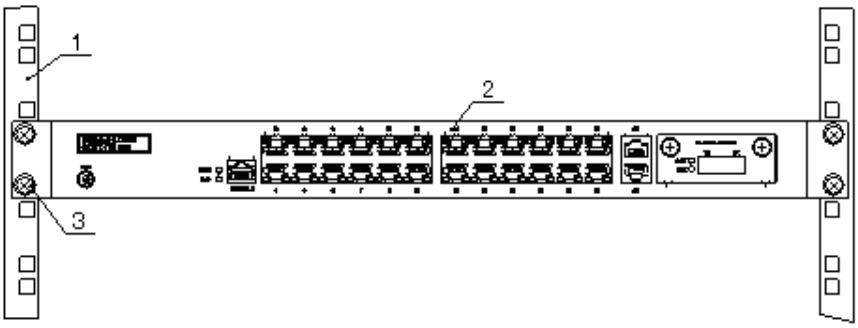
FIGURE 15 INSTALLING BRACKETS



1. Holder
2. Cabinet
3. Screw

3. After installation, push switch along with bracket, and fix flanges with screws onto cabinet, as shown in Figure 16.

FIGURE 16 FIXING THE SWITCH



1. Cabinet
2. Box
3. Screw

Installation of Cables

The following contents introduce the cable types. ZXR10 2920/2928/2952/2936-FI provides the following cables.

- Power supply cables
- Console cables
- Network cables
- Optical fibers

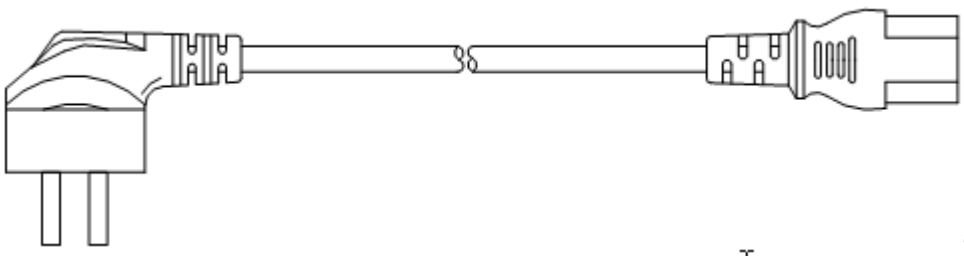
Installing Power Cables

Power cables are classified into the following two kinds of cables: AC power cables and DC power cables.

1. AC power cable installation

   An AC power cable looks the same as standard printer power cable, as shown in Figure 17.

FIGURE 17 AC POWER CABLE

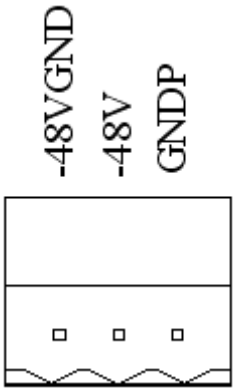


One end of AC power cable connects the AC power socket of ZXR10 2920/2928/2952/2936-FI power module. Another end of AC power cable connects the 220V AC power socket.

2. DC power cable installation

   Appearance and description of -48V power socket on DC power supply module of ZXR10 2920/2928/2952/2936-FI is shown in Figure 18.

FIGURE 18 OUTLINE DRAWING OF -48V POWER SOCKET



   DC power cable is a 3-core power cable, as shown in Figure 19.

FIGURE 19 DC POWER CABLE

   End A is plug, end B:

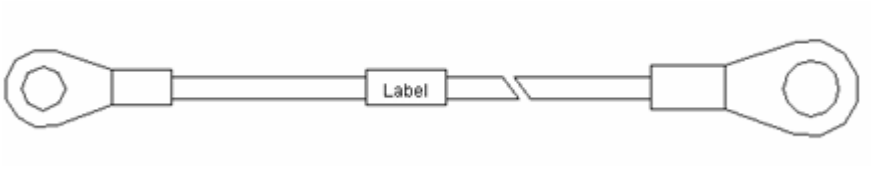
   - Blue core wire connects -48V
   - Brown core wire connects -48VGND
   - Yellowgreen core wire connects GNDP

   One end of the DC power cable is connected to the power socket on the DC power supply module of ZXR10 2920/2928/2952/2936-FI, and another end connects to the corresponding terminal of –48V DC power supply.

3. Grounding cable installation

   There is a grounding screw on the back of ZXR10 2920/2928/2952/2936-FI, indicated by ⏚. When connecting with yellowgreen protection cable, connect one end of the cable to grounding screw and the other end of the cable to protective earth of cabinet. The shape of grounding protection cable is shown in Figure 20.

FIGURE 20 GROUNDING PROTECT CABLE



Installing Configuration Cables

The serial port configuration cable is used for the configuration and routine maintenance of the ZXR10 2920/2928/2952/2936-FI.

The ZXR10 2920/2928/2952/2936-FI is delivered with serial port configuration cable. One end of the cable is a DB9 serial port, which is connected with the serial port on the computer. The other end is an RJ45 port, which is connected to the Console port on the ZXR10 2920/2928/2952/2936-FI. Figure 21 shows the appearance of a configuration cable and Table 7 provides the cable pinout.

FIGURE 21 SERIAL PORT CONFIGURATION CABLE

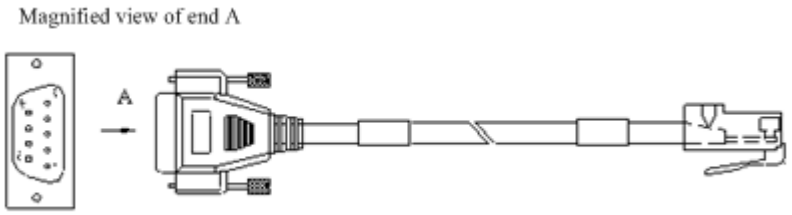


TABLE 7 PINOUT OF SERIAL PORT CONFIGURATION CABLE

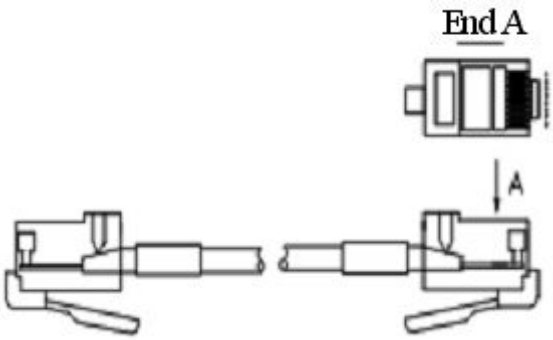
End A	Color	End B
2	White	3
3	Blue	6
5	White	4
	Orange	5
4	White	7
6	Green	2
7	White	8
8	Brown	1

Installing Network Cables

Both ends of the network cable are crimped with RJ45 connectors, as shown in Figure 22.

- Name of the cable connector: 8P8C straight cable crimping connector
- Model: E5088-001023
- Technical parameters: Rated current 1.5 A, rated voltage 125 V, and crimping round wire AWG24-28#.

FIGURE 22 STRUCTURE OF NETWORK CABLE



By the sequence of crimping the lines in the connector, the cables can be classified into:

- Straight-through cable RJ45, with one-to-one connection correspondence at two ends of the cable. The specific pinout is shown in Table 8.

TABLE 8 RJ45 PINOUT OF STRAIGHT-THROUGH CABLE

A End	Cable Colors	B End
1	White/orange	1
2	Orange	2
3	White/green	3
6	Blue	6
4	White/blue	4
5	Green	5
7	White/brown	7
8	Brown	8

- Crossover cable RJ45J with two twisted pairs at two ends of the cable corresponding to each other in the crossover mode. The specific pinout is shown in Table 9.

TABLE 9 RJ45J PINOUT OF CROSSOVER CABLE

A End	Cable Colors	B End
1	White/orange	3
2	Orange	6
3	White/green	1
6	Blue	4
4	White/blue	5
5	Green	2
7	White/brown	7
8	Brown	8

Installing Fibers

Each optical port of the ZXR10 2920/2928/2952/2936-FI is connected to two fibers: one for receiving and the other for transmission. They are respectively marked as RX and TX on the panel. Note not to insert the wrong fibers. Fibers are classified into single-mode and multi-mode fibers. You can configure 6 types of fibers as listed in Table 10 according to your application requirements.

TABLE 10 FIBER TYPES

Mode	Type of Connector on the Switch	Type of Connector on the Peer End
Single-mode fiber	SC-PC connector (square and flat head) LC-PC (small square and flat head)	FC/PC connector
		SC/PC connector
		ST/PC connector
		LC-PC connector
multi-mode fiber	SC-PC connector (square and flat head) LC-PC (small square and flat head)	FC/PC connector
		SC/PC connector
		ST/PC connector
		LC-PC connector

For fiber layout out of the cabinet, make sure to protect the fibers against any damages with plastic corrugated protection tubes. Optical fibers inside the protection tube should not entangle with one another, and they shall be bent into a round shape at the bending position, if any. The labels at the two ends of the optical fiber shall be clear and legible. The meanings of the labels shall clearly

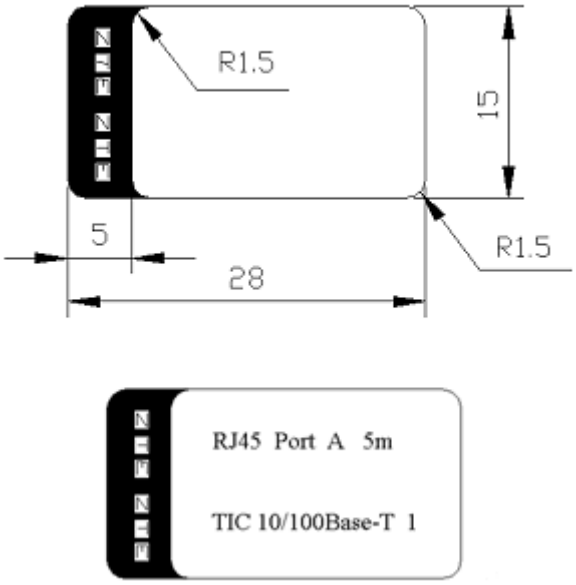
reflect the corresponding numbers and relationship between cabinets and between rows.

Labels

1. The pattern and meanings of the labels attached to the connector.

   The label attached to the connector is called transverse English label on panels and connectors. Figure 23 shows the structure and dimensions of the label.

   FIGURE 23 TRANSVERSE ENGLISH LABEL ON PANELS AND CONNECTORS



   Meanings of the contents on the labels are as follows:

   RJ45——Cable English number. The corresponding name is parallel network cable.

   Port A——End A of the cable connector, corresponding to End B or another end.

   5——Length of the finished cable. It refers to the straight line length of the cable from the connector at one end to the connector at the other end.

   TIC 10/100Base-T 1——Connection position, the first 10/100Base-T network port of the TIC board.

2. The pattern and meanings of the label attached to the cable.

   The label attached to the cable is called roll-type self-cover laser print label model II. Figure 24 shows the structure and dimensions of the label.

FIGURE 24 ROLL-TYPE SELF-COVER LASER PRINT LABEL MODEL II

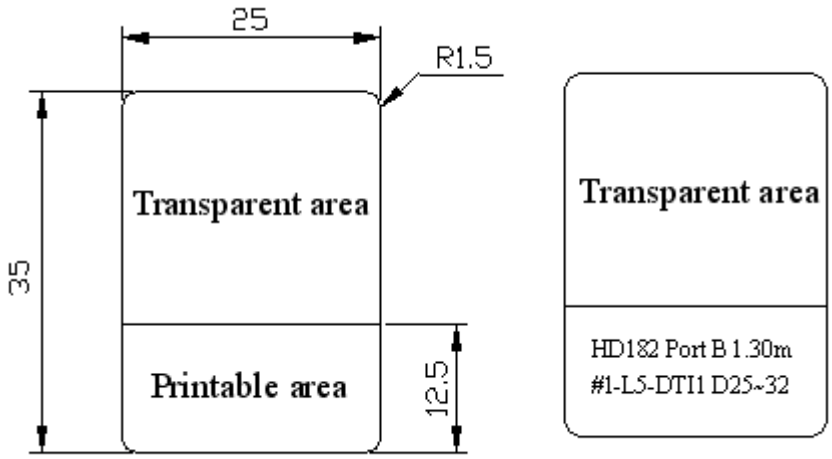
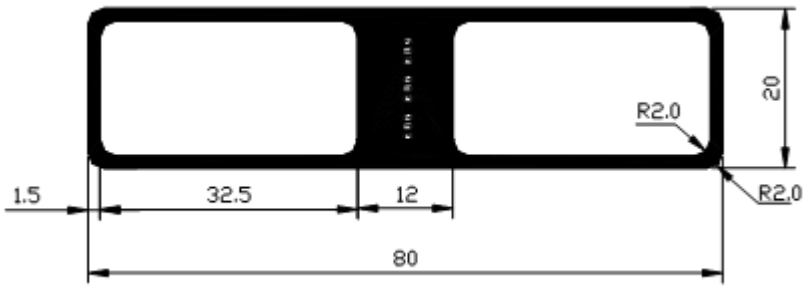


Figure 24 have the same meanings as those of the label in Figure 23. These two types of label are used in different places. The transverse English label on panels and connectors is only applicable to the connectors where the attachment area is larger than the label area or to panels. The roll-up self-mulching laser printing label is rolled around the cable with its own scotch adhesive tapes. It is used when the horizontal English label cannot be used because the cable connector is small or the cable does not look nice with a horizontal English label.

3. Before the cabinet equipment is delivered, all the internal interconnected cables shall be attached with flag-type direction labels.

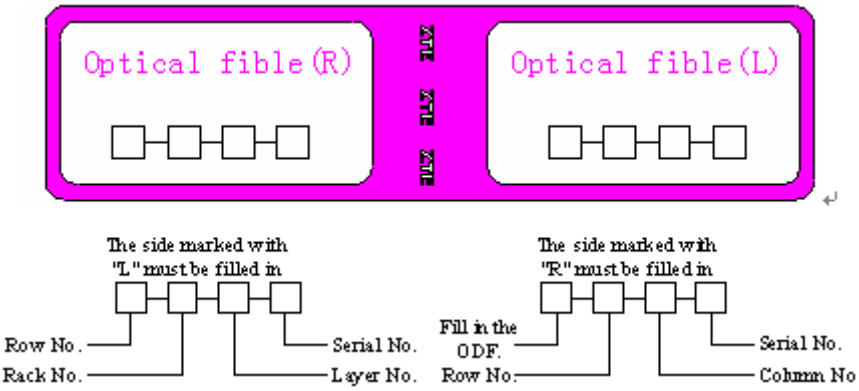
   This label attached to the cable is called Transverse English Type I Label. Figure 25 shows the structure and dimensions of the label. The contents of the label have the same meanings as those of the label in Figure 23 .

FIGURE 25 TRANSVERSE ENGLISH TYPE I LABEL



4. The meaning of the content and the structure of a fiber engineering label are as shown in Figure 26.

FIGURE 26 PATTERN AND MEANINGS OF THE ENGINEERING LABEL ON THE OPTICAL FIBER



The two sides of the engineering label on the optical fiber are marked "L" and "R" with the specific meanings as follows:

- When the label is pasted on the fiber at the ZXR10 2920/2928/2952/2936-FI side, the row number and column number of the cabinet at the side of the connected remote optical interface device as well as the layer No. of the fiber in the cabinet and the fiber No. should be filled in the R area of the label. In this case, the row No. and column No. of ZXR10 2920/2928/2952/2936-FI where the fiber is located as well as the layer No. of the fiber and fiber number shall be filled in the L area of the label.
- If the label is attached on the optical interface equipment of the customer, contents filled on the label are just contrary to those at the ZXR10 2920/2928/2952/2936-FI side.

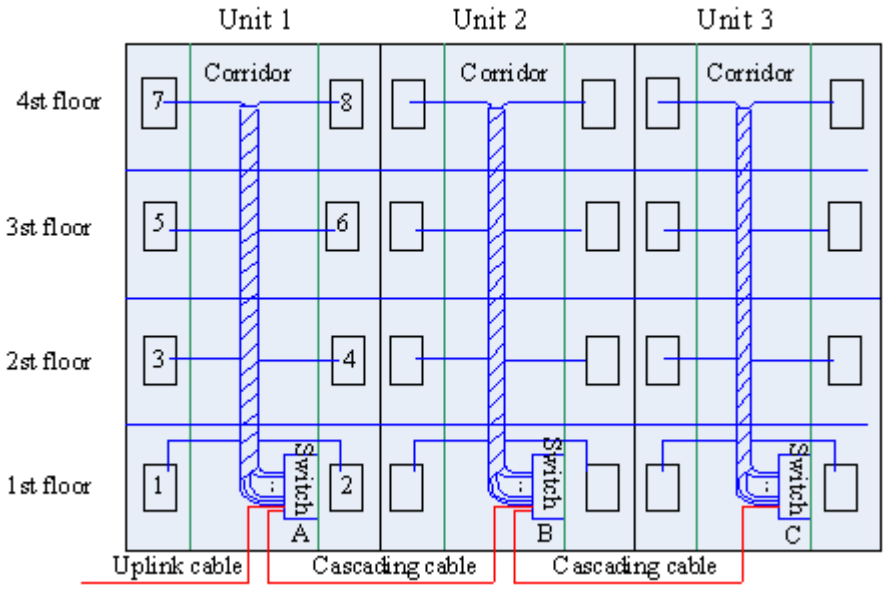
Cable Lightning Protection Requirements

According to the degree of hazard, lightning is classified into direct lightning strike and lightning induction. The damage of direct lightning strike is hard to avoid. But proper lightning protection measure can effectively prevent the lightning induction. The following lightning protection requirements are proposed to reduce the equipment failure rate in the areas where lightning is frequent.

1. The Ethernet switch shall be placed in the corridor, preferably on the first floor. To avoid the direct sunshine, rains, and lightning, the switch cannot stay in an outdoor place where no weather-proof measures are taken. Ensure that all subscriber lines, except the uplink, downlink, and cascading lines, are distributed inside the building to avoid the attack of lightning induction.

Figure 27 shows the cabling of Ethernet switch in a four-floor building with three units. Where, switch A in Unit 1 is the convergence switch of the whole building, and switches B and C are access switches. Switches A, B, and C are cascaded. That is, the cascading cable of switch A is the uplink cable of switch B, and the cascading cable of switch B is the uplink cable of switch C. The rest subscriber lines are distributed inside the building and connected to the subscriber terminals from bottom to top in the corridor.

FIGURE 27 CABLING OF THE ETHERNET SWITCH IN A BUILDING

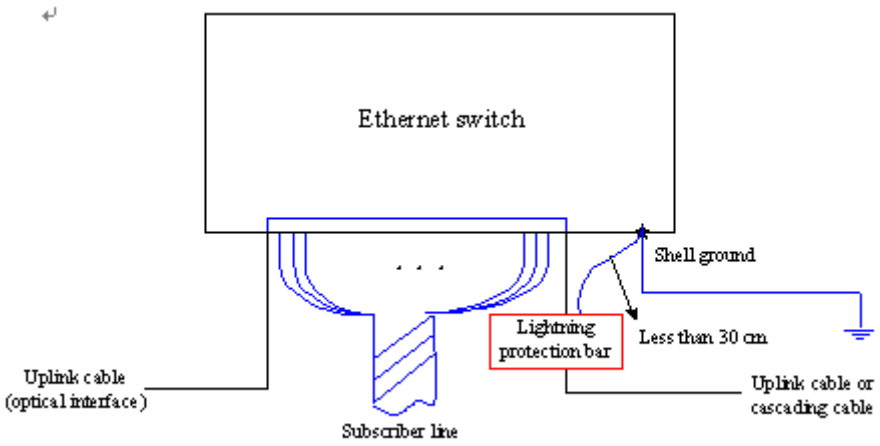


In the above figure, 1 to 8 stands for subscribers. The cascading cable refers to the cable connecting two switches.

2. Reinforced lightning protection measures must be taken and lightning protection bars must be added for the uplink, downlink, and cascading Ethernet ports that are led outdoors. In special case when the common subscriber lines must be distributed outdoors, lightning protection bars must also be added. The lightning protection capability of the lightning protection bar must reach 6 KV or above and the current discharge capability must reach 5 KA. The grounding cable of the lightning protection bar must have a diameter of 16mm^2 and a length less than 30 cm. It is recommended to use the optical port as the uplink port of the convergence switch in the building. If the electrical port is used, lightning protection bars must be added.

   Figure 28 shows the cabling of a convergence switch. Where, the uplink port is the optical port and lightning protection bars are added for the downlink or cascaded cables. The lightning bars are connected to the earth through the shell. The rest subscriber lines are distributed inside the building.

FIGURE 28 CABLING OF A CONVERGENCE SWITCH



3. The grounding system with good ground grid is preferred for the switch. A lot of residential buildings with proper grounding have a grounding resistance of 1 ohm. If the test shows that grounding system is not satisfied, it is recommended to equip an independent grounding post and the grounding cable must be 16 mm^2 in diameter and as short as possible. Whichever grounding method is used, the grounding resistance must be less than 5 ohm and cannot exceed 10 ohm.
4. It is prohibited that the switch directly gets the power from the outdoor overhead power cable. If the switch must directly get the power from the outdoor overhead power cable, special lightning protection measures, such as lightning protection socket and lightning protection bar, must be added to the power supply. The lightning protection bar for the power supply must have better lightning protection index than that for the port cable.
5. Whether the Ethernet switch will suffer lightning strike is affected by a lot of factors, including grounding, power supply, and wiring. The lightning strike lead-in mechanism also varies a lot. Taking one measure is far from enough to prevent the lightning strike. Therefore, several measures must be implemented at the same time. Proper grounding, appropriate power supply, reasonable wiring, and suitable lightning protection measures will definitely reduce the chance of the switch damage resulted from lighting strike.

System Debugging

Connection Configuration

The ZXR10 2920/2928/2952/2936-FI debugging is implemented through the Console. The Console port connection configuration

adopts the VT100 terminal mode. The following takes the configuration of HyperTerminal provided by the Windows operating system as an example.

1. Select **Start > Programs > Accessories > Communications > HyperTerminal**, on the PC screen to start the HyperTerminal, as shown in Figure 29 .

FIGURE 29 STARTING THE HYPERTERMINAL

2. Input the related local information in the interface as shown in Figure 30.

FIGURE 30 LOCATION INFORMATION

Location Information
Before you can make any phone or modem connections, Windows needs the following information about your current location.
What country/region are you in now?
China
What area code (or city code) are you in now?
025
If you dial a number to access an outside line, what is it?
4826606
The phone system at this location uses:
Tone dialing
Pulse dialing
OK
Cancel

3. After the **Connection Description** dialog box appears, enter a name and choose an icon for the new connection, as shown in Figure 31.

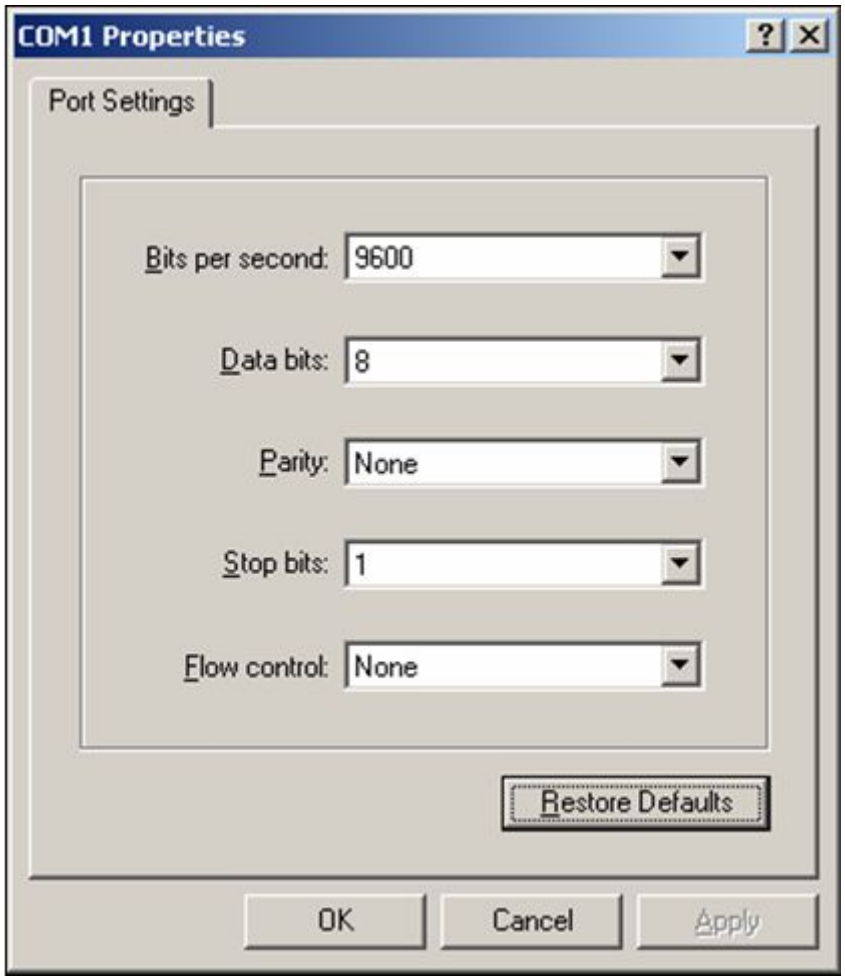
FIGURE 31 SETTING UP A CONNECTION

4. Based on serial port connection to the console cable, choose COM1 or COM2 as the serial port to be connected, as shown in Figure 32 .

FIGURE 32 CONNECTION CONFIGURATION

5. Enter the properties of the selected serial port as shown in Figure 33 . The port property configuration includes: Bits per Second 9600, Data bit 8, Parity None, Stop bit 1, Data flow control None.

FIGURE 33 COM1 PROPERTIES



Power on and boot ZXR10 2920/2928/2952/2936-FI to initialize the system and to enter into configuration for operational use.

Power-on Procedure

Before powering on the ZXR10 2920/2928/2952/2936-FI, check the environment in the equipment room and the hardware installation.

1. Check whether the temperature, humidity, and voltage of the power supply in the equipment room meet the requirements listed in Table 11 .

TABLE 11 TEMPERATURE AND HUMIDITY TABLE

Check Item	Temperature℃		Relative Humidity%	
	Long-term Working Condition [3]	Short-term Working Condition [4]	Long Term Operating Condition	Short Term Operating Condition
Range	15 ℃~30 ℃	-5 ℃~45 ℃	30%~70%	20%~90%

2. Check whether the power cables and other cables are correctly and reliably connected.
3. Check other hardware conditions.
   i. Equipment labels shall be complete, correct and legible.
   ii. Equipment is installed reliably in the 19” standard cabinet.
   iii. The power switch of the equipment is turned off.
   iv. The rack is properly grounded, with the grounding resistance meeting relevant technical requirements.

To power on the 2920/2928/2952/2936-FI, do as follows:

1. Turn on the external power supply.
2. Turn on the power switch at the back of the switch.

To power off the 2920/2928/2952/2936-FI, do as follows:

1. Turn off the power switch at the back of the switch.
2. Turn off the external power supply.

Indicator Status

After the switch is powered on, the system indicators change in the following way:

1. After the system is powered on, the PWR indicator is on and the RUN indicator is flashing.
2. The BootROM starts to load the version. If the version is unavailable, the states of indicators do not change. If the version is loaded normally, the RUN indicator flashes at 1 Hz.

System Boot Procedure

The procedure to start the system is as follows:

3. In normal working environment of the ZXR10 2920/2928/2952/2936-FI, the temperature and humidity are measured 2m above the floor and 0.4m in front of the equipment when the front and rear protection boards are removed.
4. The short-term working condition means that the continuous running period is no more than 48 hours, and the accumulated running period in a year is no more than 15 days.

After the system is powered on, start the hardware. After the hardware test is passed, the following information appears on the management terminal:

```
Welcome to use ZTE eCarrier!!



Copyright(c) 2004-2006,  ZTE Co., Ltd.
System Booting......
CPU: DB-88E6218
BSP version: 1.2/6-b
Creation date: Jan  3 2008, 11:46:44



Press any key to stop auto-boot...
7
```

After the above information appears, wait for about 7 seconds and then press any key to enter the boot status. Then modify the startup parameters. If the system does not detect any input within the specified time, the system begins to automatically load the version and displays the following information:

```
auto-booting...


boot device          : marfec
unit number          : 0
processor number     : 0
host name            : f129750
file name            : kernel
inet on ethernet (e) : 10.40.89.106
host inet (h)        : 10.40.89.78
gateway inet (g)     : 10.40.89.78
user (u)             : 2952
ftp password (pw)    : 2952
flags (f)            : 0x0
other (o)            : MAC0-00:32:45:67:89:ab

Attaching to TFFS... done.
Loading file :kernel
Uncompressing...
Uncompressed 4273428 bytes Ok.
Loading image... 12720656
Starting at 0x10000...

Attached TCP/IP interface to marfec unit 0
Attaching interface lo0...done


------------------------------------------------------------------------------
    The switch's mac address is:00.d0.d0.fa.29.20
    Module 0: ZXR10 2952-SI; fasteth: 48; gbit: 0;
    Module 1: COPPER 1000M; fasteth:  0; gbit: 1;
    Module 2: COPPER 1000M; fasteth:  0; gbit: 1;
    Module 3: FIBER 1000M; fasteth:  0; gbit: 1;
    Module 4: FIBER 1000M; fasteth:  0; gbit: 1;
    Software Version Number: v2.0.11.V
    Software Version Date  : Jan  3 2008  18:59:10
    Flash file system initializing...
    Flash file system initialize passed
    Config system begin ...
      Switch Start (70) config 1 row success
      Switch Portmap (71) config 68 row success
      Switch Global (72) config 1 row success
Switch Port (73) config 52 row success
      Switch VLAN (74) config 4094 row success
      Switch TRUNK (75) config 15 row success
      Switch End (79) config 1 row success
      Switch Global 1.0.1 (126) config 1 row success
      LACP (80) config 1 row success
```

```
      Igmp Filter (83) config 1 row success
      Igmp Snooping (84) config 1 row success
      Vlan Jump (85) config 1 row success
      Mstp bridge information (292) config 1 row success
      Mstp Instance information (293) config 1 row success
      Mstp port_instance information (294) config 1 row success
      Loopback detection (88) config 1 row success
      IP bind VLAN (15) config 1 row success
      IP port (10) config 64 row success
      Static ARP (12) config 1 row success
      RIP (30) config 1 row success
      Certify (60) config 1 row success
      Sdp (120) config 1 row success
      Snmp Community (140) config 1 row success
      Snmp View (141) config 1 row success
      Snmp Trap (143) config 1 row success
      Rfc1213 System Group (144) config 1 row success
      Rfc1493 config (146) config 1 row success
      Snmp v3 engine (153) config 1 row success
      Rmon enable or disable (174) config 1 row success
      Radius basic config (201) config 1 row success
      Login authentication config (203) config 1 row success
      SSH V2.0 (125) config 1 row success
      Web server config (128) config 1 row success
      Dot1x config (205) config 1 row success
      Iptv global config (206) config 1 row success
      Iptv preview config (207) config 1 row success
      Iptv CDR config (208) config 1 row success
      Iptv viewprofile config (209) config 1 row success
      Iptv package config (211) config 1 row success
      Dot1x special access config (213) config 1 row success
      Zdp config (231) config 1 row success
      Ztp config (232) config 1 row success
      Group management config (233) config 1 row success
Switch QoS global configure (261) config 1 row success
      Switch QoS port configure (262) config 52 row success
      Switch Syslog parameter configure (311) config 1 row success
      Switch PvlanTable configure (89) config 1 row success
      Switch Qinq parameter configure (301) config 1 row success
      Switch NTP parameter configure (321) config 1 row success
      GARP (330) config 1 row success
      GVRP Port parameter configure (331) config 1 row success
      Switch vbas configure (90) config 1 row success
      SFLOW parameter configure (340) config 1 row success
      Switch time range configure (351) config 1 row success
      Switch acl group configure (352) config 1 row success
      Switch acl port configure (354) config 1 row success
      DHCP configure (92) config 1 row success
      L2PT configure (94) config 1 row success
      Ethernet OAM global configure (371) config 1 row success
      Ethernet OAM port configure (372) config 1 row success
      VLAN translation configure (95) config 1 row success
    Config system end


Welcome !
ZTE Corporation.
All rights reserved.


login:
```

After the system is started successfully, the prompt character "login:" is displayed, requesting you to input the login user name and password. The default user name is admin and password is zhongxing.

This page is intentionally blank.

Chapter 5

Usage and Operation

Table of Contents

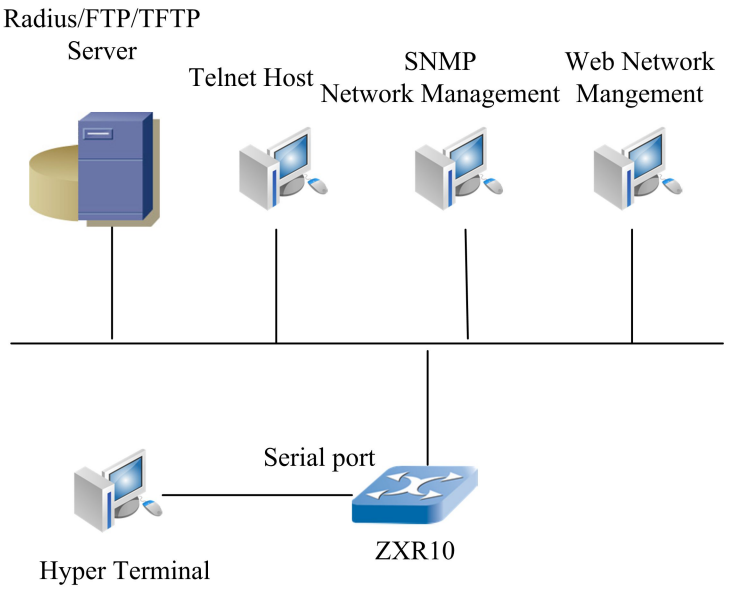
Configuration Modes 43
Command Mode 47
Usage of Command Line 51

Configuration Modes

ZXR10 2920/2928/2952/2936-FI provides several configuration modes. As shown in Figure 34 , select a configuration mode according to the network connected.

1. Configuration through Console port connection
2. Configuration through TELNET session
3. Configuration through SSH connection
4. Configuration through SNMP connection
5. Configuration through WEB connection

FIGURE 34 ZXR10 2920/2928/2952/2936-FI CONFIGURATION MODES



Configuration through Console Port Connection

Configuration through console port connection is the main configuration mode of the ZXR10 2920/2928/2952/2936-FI. For the operation procedure, refer to Connection Configuration. The user can also configure the connection when the equipment is running.

Configuration through TELNET Session

Telnet mode is often used for configuring a remote switch. The user can log in to the remote switch through the Ethernet port of the local host. The login username and password must be configured on the switch and ping the IP address of the layer 3 port on the switch successfully on the local host. (For configuration of IP address of the layer 3 port, see Configuring IP Port.)

Use the command **create user** <*name*>{**admin** | **guest**} (the length of username does not exceed 15 characters) to create a new management user, the command **set user local** <*name*> **login-password** [<*string*>] (the length of login-password does not exceed 16 characters) to set the login password.

Use the command **set user** {**local** | **radius**}<*name*> **admin-password** <*string*> (the length of admin-password does not exceed 16 characters) to set administrator password.

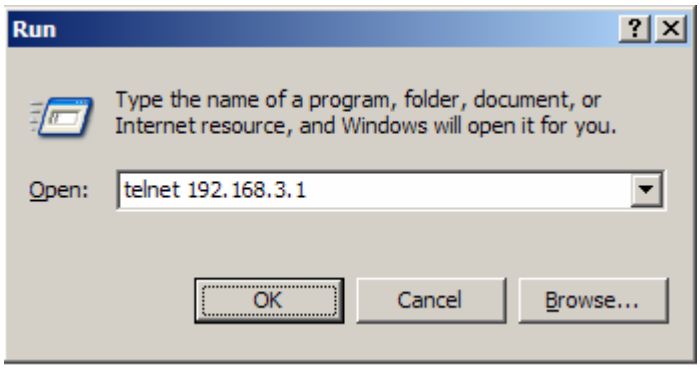
Note:

The default username is admin and the password is zhongxing. The default management password is null.

Suppose the IP address of the layer 3 port is 192.168.3.1 and this address can be pinged from the local host. Then perform the remote configuration as follows:

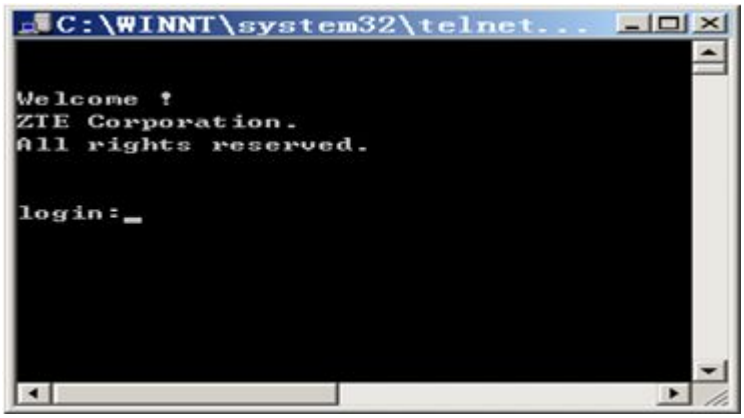
1. Run the Telnet command on the host, as shown in Figure 35.

FIGURE 35 RUNNING THE TELNET



2. Click **OK**, a Telnet window appears, as shown in Figure 36.

FIGURE 36 SWITCH REMOTE LOGIN WINDOW



3. Enter the username and password to enter the user mode of the switch.

Configuration through SSH Connection

Telnet and FTP connections are not safe because they use the plain text to transmit the password and data on the network. This results in data to be easily intercepted by attackers. A disadvantage of the Telnet/FTP security authentication is that it is easily attacked by the man-in-the-middle. This imitates the server to receive the data sent by the client and imitates the client to transmit the data to the real server.

SSH can solve this hidden trouble. The SSH sets up a security channel for the remote login on non-security network and other network to encrypt and compress all transmitted data. In this way, no useful information can be obtained in the interception.

The detailed SSH configuration of the ZXR10 2920/2928/2952/2936-FI refers to Basic Configuration of SSH.

Configuration through SNMP Connection

Simple Network Management Protocol (SNMP) is the most popular network management protocol. The user can use one NM server to manage all the equipments on the network through this protocol.

SNMP adopts the server/client-based management mode. The background NM server serves as an SNMP server, and the foreground network equipment, the ZXR10 2920/2928/2952/2936-FI serves as the SNMP client. The foreground and background share the same MIB management database and communicate with each other via the SNMP.

The background NM server must be installed with the NM software that supports SNMP. The management and configuration of the ZXR10 2920/2928/2952/2936-FI are implemented through the NM software. For the SNMP configuration on the ZXR10 2920/2928/2952/2936-FI refer to Basic Configuration of SNMP.

Configuration through WEB Connection

Web is another way to implement remote management of switch and is similar with Telnet. The user can log in to the remote switch through the Ethernet port of the local host. The login username, login password and administrator password must be configured on the switch and then enable Web function. Also ping the IP address of the layer 3 port on the switch successfully on the local host.For configuration of IP address of the layer 3 port, see Layer 3 Basic Configuration.

1. Create a new management user

   create user <*name*>{**admin** | **guest**}

   user <*name*>: the length cannot exceed 15 characters.

2. Configure login password

   set user local <*name*> **login-password** <*string*>

   login-password <*string*>the length cannot exceed 16 characters.

3. Configure administrator password

   set user {**local**|**radius**}<*name*> **admin-password** <*string*>

   admin-password <*string*>: the length cannot exceed 16 characters.

4. Enable web network management function (by default, this function is disabled) and set listening port.

   set web enable

   set web listen-port < *80,102549151* >

Note:

The default username is admin and the password is zhongxing. The administrator password is empty. If login with administrator account number, administrator password cannot be empty. Therefore set administrator password first. The default http listening port is 80.

The detailed web remote logging and configuration refer to Configuring System Login.

Command Mode

To facilitate the configuration and management of the switch, the commands of the ZXR10 2609/2809/2818S/2826S/2852S are allocated to different modes according to the functions and authorities. A command can be executed only in the specified mode. The ZXR10 2609/2809/2818S/2826S/2852S command modes include:

1. User mode
2. Global configuration mode
3. SNMP configuration mode
4. Layer 3 configuration mode
5. File system configuration mode
6. NAS configuration mode
7. Cluster management configuration mode
8. Basic ACL configuration mode
9. Extended ACL configuration mode
10. Layer 2 ACL configuration mode
11. Hybrid ACL configuration mode
12. Global ACL configuration mode

User Mode

When you log in to the switch through the HyperTerminal or Telnet, you can enter the user mode after entering the login username and password. The prompt character in the user mode is the host name followed by ">" as shown below:

```
zte>
```

The default host name is zte. The user can modify the host name by using the command **hostname** <*name*>.

In the user mode, you can execute the command **exit** to exit the switch configuration or execute the command **show** to display the system configuration and operation information.

Note:

The command **show** can be executed in any mode.

Global Configuration Mode

In the user mode, enter the **enable** command and the corresponding password to enter the global configuration mode, as follows:

```
zte>enable
Password:***
zte(cfg)#
```

In the global configuration mode, you can configure various functions of the switch. Thus, use the command **set user** <*name*> **admin-password** [<*string*>] to set the password for entering the global configuration mode to prevent the login of unauthorized users.

To return to the user mode from the global configuration mode, use the **exit** command.

File System Configuration Mode

In the global configuration mode, execute the command **config tffs** to enter the file system configuration mode, as shown below:

```
zte(cfg)#config tffs
zte(cfg-tffs)#
```

In the file system configuration mode, you can operate on the switch file system, including adding file directory, deleting file or directory, modifying file name, displaying file or directory, changing file directory, uploading/downloading files through TFTP, copying files, formatting Flash, and so on.

To return to the global configuration mode from the file system configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Layer 3 Configuration Mode

In the global configuration mode, execute the command **config router** to enter the layer 3 configuration mode, as shown in the following example:

```
zte(cfg)#config router
zte(cfg-router)#
```

In the Layer 3 configuration mode, the user can configure the Layer 3 port, static router, and ARP entities.

To return to the global configuration mode from the layer 3 configuration mode, use the command **exit** or press **<Ctrl+Z>**.

NAS Configuration Mode

In the global configuration mode, execute the command **config nas** to enter the NAS configuration mode, as shown below:

```
zte(cfg)#config nas
zte(cfg-nas)#
```

In the NAS configuration mode, the user can configure the switch access service, including the user access authentication and management.

To return to the global configuration mode from the NAS configuration mode, use the command **exit** or press **<Ctrl+Z>**.

SNMP Configuration Mode

In the global configuration mode, you can use the command **c onfig snmp** to enter the SNMP configuration mode, as shown below:

```
zte(cfg)#config snmp
zte(cfg-snmp)#
```

In the SNMP configuration mode, you can set the SNMP and RMON parameters.

To return to the global configuration mode from the SNMP configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Cluster Management Configuration Mode

In the global configuration mode, execute the command **config group** to enter the cluster management configuration mode, as shown below:

```
zte(cfg)#config group
zte(cfg-group)#
```

In the cluster management configuration mode, you can configure the switch cluster management service.

To return to the global configuration mode from the cluster management configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Basic ACL Configuration Mode

In the global configuration mode, execute the command **config acl basic number** <*1-99*> to enter basic ACL configuration mode, as shown below:

```
zte(cfg)#config acl basic number 10
zte(basic-acl-group)#
```

In the basic ACL configuration mode, you can add, delete and move the rules of basic ACL with specific ACL number .

To return to the global configuration mode from basic ACL configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Extended ACL Configuration Mode

In the global configuration mode, execute the command **config acl extend number** <*100-199*> to enter extended ACL configuration mode, as shown below:

```
zte(cfg)#config acl extend number 100
zte(extend-acl-group)#
```

In the extended ACL configuration mode, you can add, delete and move the rules of extended ACL with specific ACL number.

To return to the global configuration mode from extended ACL configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Layer 2 ACL Configuration Mode

In the global configuration mode, execute the command **config acl link number** <*200-299*> to enter layer 2 ACL configuration mode, as shown below:

```
zte(cfg)#config acl link number 200
zte(link-acl-group)#
```

In the layer 2 ACL configuration mode, you can add, delete and move the rules of layer 2 ACL with specific ACL number.

To return to the global configuration mode from layer 2 ACL configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Hybrid ACL Configuration Mode

In the global configuration mode, execute the command **config acl hybrid number** <*300-399*> to enter hybrid ACL configuration mode, as shown below:

```
zte(cfg)# config acl hybrid number 333
zte(hybrid-acl-group)#
```

In the hybrid ACL configuration mode, you can add, delete and move the rules of hybrid ACL with specific ACL number.

To return to the global configuration mode from hybrid ACL configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Global ACL Configuration Mode

In the global configuration mode, execute the command **config acl global** to enter global ACL configuration mode, as shown below:

```
zte(cfg)#config acl global
zte(global-acl-group)#
```

In the global ACL configuration mode, you can add, delete and move the rules of global ACL with specific ACL number.

To return to the global configuration mode from global ACL configuration mode, use the command **exit** or press **<Ctrl+Z>**.

Usage of Command Line

Online Help

In any command mode, enter a question mark (?) behind the DOS prompt of the system, a list of available commands in the command mode will appear. You can use the online help to get keywords and parameter list of any command.

1. In any command mode, enter a question mark "?" behind the DOS prompt of the system, and a list of all commands in the mode and the brief description of the commands will appear. For example:

```
zte>?
  enable              enable configure mode
  exit                exit from user mode
  help                description of the interactive help system
  show                show config information
  list                print command list
zte>
```

2. Input a question mark behind a character or string, commands or a list of keywords starting with the character or string can be displayed. Note that there is no space between the character (string) and the question mark. For example:

```
zte(cfg)#c?
config  clear  create
zte(cfg)#c
```

3. Input a question mark behind a command, a keyword or a parameter, the next keyword or parameter to be input will be

listed, and also a brief explanation will be given. Note that a space must be entered before the question mark. For example:

```
zte(cfg)#config ?
  snmp                enter SNMP config mode
  router              enter router config mode
  tffs                enter file system config mode
  nas                 enter nas config mode
  group               enter group management config mode
  acl                 enter acl config mode
zte(cfg)#config
```

4. If you enter a wrong command, keyword, or parameter and press Enter, the message "Command not found" will be displayed on the interface. For example:

```
zte(cfg)#conf ter
  %  Command not found (0x40000066)
zte(cfg)#
```

Example In the following example, the online help is used to help create a username.

```
zte(cfg)#cre?
create
zte(cfg)#create ?
  port                create descriptive name for port
  vlan                create descriptive name for vlan
  user                create user
zte(cfg)#create user
  %  Parameter not enough (0x40000071)
zte(cfg)#create user ?
  <name >             user name<length<=15>
zte(cfg)#creat user wangkc ?
  admin               create an administrator
  guest               create a guest
zte(cfg)#creat user wangkc guest ?
  <cr>
zte(cfg)#creat user wangkc guest
```

Command Abbreviations

In the ZXR10 2920/2928/2952/2936-FI, a command or keyword can be shortened into a character or string that can uniquely identify this command or keyword. For example, the command **exit** can be shortened as **ex**, and the command **show port** shortened as **sh por**.

History Command

The user interface supports the function of recording input commands. A maximum of 20 history commands can be recorded. The function is very useful in re-invoking of a long or complicated command.

To re-invoke a command from the record buffer, do one of the following.

Command	Function
<Ctrl+P> or **<- >**	Invoke a history command in the buffer forward
<Ctrl+N> or **<¯>**	Invoke a history command in the buffer backward

Functional Key

The ZXR10 2920/2928/2952/2936-FI provides a lot of functional keys for the user interface to facilitate user operations. Table 12 lists the functional keys.

TABLE 12 FUNCTIONAL KEYS

Functional Key	Usage
<Ctrl+P> or **<- >**	Recover the last command (Roll back in the historical records of commands).
<Ctrl+N> or **<- >**	Recover the next command (Roll forward in the historical records of commands).
<Ctrl+B> or **<¬ >**	Move left in the command line currently indicated by the prompt.
<Ctrl+F> or **<® >**	Move right in the command line where the prompt is currently located.
Tab	Display commands starting with the character or string. If there is only one command, make this command a complete one.
<Ctrl+A>	Skip to the beginning of the command line.
<Ctrl+E>	Skip to the end of the command line.
<Ctrl+K>	Delete the characters from the cursor to the end.
Backspace or**<Ctrl+H>**	Delete the character on the left of the cursor.
<Ctrl+C>	Cancel the command and display the prompt character.
<Ctrl+L>	Clear screen.
<Ctrl+Y>	Recover the last command executed.
<Ctrl+H>	Return to the global configuration mode.

When the command output exceeds one page, the output is split into several pages automatically and the prompt "----- more ----- Press **Q** or **<Ctrl+C>** to break -----" appears at the bottom of the

current page. You can press any key to turn pages or press **Q** or **<Ctrl+C>** to stop the output.

Chapter 6

System Management

Table of Contents

File System Management 55
FTP Configuration 57
Import and Export of Configuration 59
Backup and Recovery of Files 59
Software Version Upgrade 60

File System Management

File System Introduction

In the ZXR10 2920/2928/2952/2936-FI, the FLASH memory is the major storage device. Both the version file and configuration file of the switch are saved in the FLASH memory. Operations, such as version upgrading and configuration saving, should be conducted in the FLASH memory.

- The name of the version file is kernel.z.
- The name of the configuration file is running.cfg.
- The name of configuration file in text mode is config.txt.

File System Operation

Configuration Task Overview

ZXR10 2920/2928/2952/2936-FI provides many commands for file system operations. Execute the following configuration on the switch.

1. Directory Operation
2. File Operation
3. TFTP download/ upload version
4. Format FLASH

Directory Operation

The directory can be created, deleted. The current working directory, the file of the specified directory can be viewed.

Configure directory operation at global mode.

Step	Command	Function
1	zte(cfg)#**config tffs**	This enters into file system configuration mode.
2	zte(cfg-tffs)#**md** <*name*>	This creates directory.
3	zte(cfg-tffs)#**rename** < *name*>< *name*>	This modifies directory name.
4	zte(cfg-tffs)#**cd** <*directory name*>	This changes the current directory, and enters into this directory.
5	zte(cfg-tffs)#**ls**	This lists the current directories.

Use the command **remove** <*name*> to delete the specified directory.

File Operation

The file system can delete specified file, rename file name, copy file and view file information.

Configure file operation at the global configuration mode.

Step	Command	Function
1	zte(cfg)#**config tffs**	This enters into file system configuration mode.
2	zte(cfg-tffs)#**rename** < *name*>< *name*>	This changes file name.
3	zte(cfg-tffs)#**copy** <*source-pathname*><*dest-pathname*>	This copies file.
4	zte(cfg-tffs)# **ls**	This lists the current file.

Use the command **remove** <*name*> to delete the specified file.

Downloading/Uploading Version by TFTP

TFTP can be used to backup and recover the switch version file and configuration file. To download or upload version by TFTP, perform the following steps.

Step	Command	Function
1	zte(cfg)#**config tffs**	This enters into file system configuration mode.
2	zte(cfg-tffs)#**tftp** *<A.B.C.D>*{**download** | **upload**}*<name>*	This downloads and uploads version by TFTP.

Formatting FLASH

Step	Command	Function
1	zte(cfg)#**config tffs**	This enters into file system configuration mode.
2	zte(cfg-tffs)#**format**	This formats FLASH.

Caution:

After formatting the FLASH, all system software and configurations will be cleared.

FTP Configuration

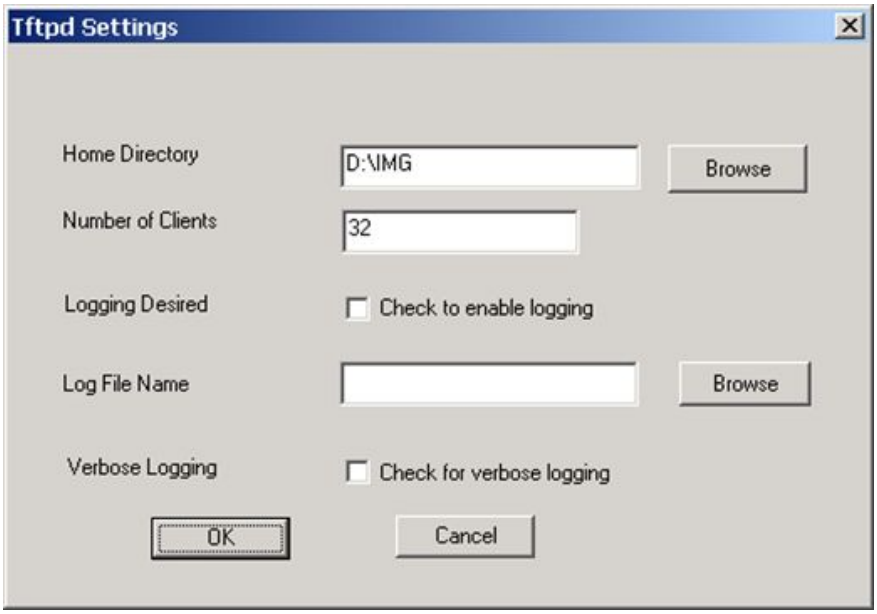
The switch version file and configuration file can be backed up or restored by TFTP. The TFTP server application software is started at the background to communicate with the ZXR10 2920/2928/2952/2936-FI (TFTP client) to implement the file backup and recovery.

1. Run the tftpd software at the background host. The interface is shown in Figure 37.

FIGURE 37 TFTPD INTERFACE

2. Click **Tftpd > Configure**, in the dialog box that appears, click **Browse** and select the directory for the version file or configuration file, for example, D:\IMG.
3. Click the second **Browse** to select log file name, click **OK** to complete the configuration. The dialog is show as Figure 38.

FIGURE 38 TFTPD SETTINGS DIALOG BOX



After the TFTP configuration is completed, perform the TFTP operations on the switch. For details, see the later sections.

Import and Export of Configuration

The ZXR10 2920/2928/2952/2936-FI provides the import and export functions of configuration information, which makes it easy to configure and manage the switch.

1. Export the configuration information

   Use the command **show running-config toFile** to export the execution result of **show running-config** to a config.txt and save it in the FLASH memory. This file can also be uploaded to the TFTP server for viewing.

   ```
   zte(cfg-tffs)#tftp 192.168.1.102 upload config.txt
   ```

2. Import the configuration information

   Running.cfg is a binary configuration file in flash and is generated by using the command **saveconfig** . Config.txt is a text-format configuration file and is generated by using the command **show running-config toFile**. Contents of the config.txt can be edited manually as needed and then downloaded to the switch by using the command **tftp**. After the configuration file is downloaded into the flash of switch, reboot the switch to import the configuration.

   ```
   zte(cfg-tffs)#tftp 192.168.1.102 download config.txt
   ```

In normal case, during the rebooting process of switch, use running.cfg file to recover the configuration. If switch can't find running.cfg, switch will check if config.txt exists, if so, switch will use this file to recover the configuration.

Backup and Recovery of Files

The files mentioned here refer to the configuration file and version file in the FLASH memory.

1. Back up the configuration file

   When a command is used to modify the switch configuration, the data is running in the memory in real time. When the switch is restarted, all the contents newly configured will be lost. Thus, you need to execute the command **saveconfig** to save the current configuration into the FLASH memory. The following shows the **saveconfig** command:

   ```
   zte(cfg)#saveconfig
   ```

To prevent damage to the configuration data, back up the configuration data by using the command tftp.

The following command can be used to back up a configuration file in the FLASH memory to the background TFTP Server:

```
zte(cfg-tffs)#tftp 192.168.1.102 upload running.cfg
```

Also can use the command **show running-config toFile** to write the configuration information into the config.txt and then back up the file to the TFTP server. For detailed method, refer to import and export of configuration.

2. Recover the configuration file

   Execute the following command to download the configuration file in the background TFTP server to the FLASH memory

   ```
   zte(cfg-tffs)#tftp 192.168.1.102 download running.cfg
   ```

3. Back up the version file

   Similar to the configuration file, you can use the command **tftp** to upload the foreground version file to the background TFTP server. For example:

   ```
   zte(cfg-tffs)#tftp 192.168.1.102 upload kernel.z
   ```

4. Recover the version file

   Version file recovery is used to retransmit the background backup version file to the foreground through TFTP. Recovery is very important in the case of upgrade failure. The version recovery operation is basically the same with the version upgrade procedure. For details, refer to software version upgrade.

Software Version Upgrade

Normally, version upgrading is needed only when the original version does not support some functions or the equipment cannot run normally due to some special reasons. Improper version upgrade operation may result in upgrade failure and startup failure of the system. Therefore, before version upgrading, the maintenance personnel shall be familiar with the principles and operations of the ZXR10 2920/2928/2952/2936-FI and master the upgrading procedure.

Version upgrade can be carried out in one of the following cases: When the operation of switch system is normal and when the operation of the switch system is abnormal.

Viewing the Version Information

If the system state allows, check the version information before and after the upgrade.

In the global configuration mode, execute the command **show version** to display the system hardware and software version information.

The displayed contents are as follows:

```
zte(cfg)#show version
    ZXR10 Router Operating System Software, ZTE Corporation:
    ZXR10 Version Number   : 29SI Series v2.0.11.V
    Copyright (c) 2001-2007 By ZTE Corporation
    Compiled: 18:59:10 Jan  3 2008
    System uptime is  0 years 0 days 0 hours 6 minutes 11 seconds

    Main processor      : MARVELL 6218
    Bootrom Version     : v1.0       Creation Date : 2008.1.9
    System Memory       : 32 M bytes System Flash  : 4 M bytes
    EPLD Version (Dno.) : v1.0       FPGA Version (Dno.): NONE
    Switch's Mac Address: 00.d0.d0.fe.29.52

      Module 0:      ZXR10 2952-SI; fasteth: 48; gbit: 0;
      Module 1:       COPPER 1000M; fasteth:  0; gbit: 1;
      Module 2:       COPPER 1000M; fasteth:  0; gbit: 1;
      Module 3:        FIBER 1000M; fasteth:  0; gbit: 1;
      Module 4:        FIBER 1000M; fasteth:  0; gbit: 1;
    zte(cfg)#
```

Version Upgrade When the System is Normal

If the switch runs normally, upgrade the version as follows:

1. Connect Console port of the switch to the serial port of the background host using the self-contained configuration cable. Connect an Ethernet port of the switch to the network port of the background host using a network cable. Check whether the connections are correct.
2. Set the IP address of the Ethernet port on the switch. Set the IP address of the background host used for upgrade. The two IP addresses must be in the same network segment so that the host can **ping** the switch.
3. Start the TFTP server software on the background host and configure it by referring to FTP Configuration.
4. On the switch, use the command **show version** to check the information of current operating version.
5. Enter the file system configuration mode and execute the command **remove** to delete the old version file in the FLASH memory. If the FLASH memory has sufficient space, change the name of the old version file and keep it in the FLASH memory.

   ```
   zte(cfg)#config tffs
   zte(cfg-tffs)#remove kernel.z
   ```

6. Use the command **tftp** to upgrade the version. The following shows how to download the version file from the TFTP server to the FLASH memory:

   ```
   zte(cfg-tffs)#tftp 192.168.1.102 download kernel.z
   ............................................................
     1, 979, 157 bytes downloaded
   zte(cfg-tffs)#
   ```

7. Restart the switch. After successful startup, check the version under running and confirm whether the upgrading is successful.

Note:

When version upgrades, especially when remote version upgrades, the compatibility problem of new and old versions appears. Generally, binary configuration file running.cfg compatibility is bad, so it is recommended that test the configuration recovery first and then decide if config.txt need to be used for recovery. If version span is large, use config.txt for recovery. After upgrading, check if the recovered configuration is the same as the original one. If not, configure according to the actual situation to avoid configuration fault caused by upgrade.

Version Upgrade When the System is Abnormal

When the switch cannot be started normally or runs abnormally, upgrade the version as follows:

1. Connect Console port of the switch to the serial port of the background host by using the self-contained configuration cable. Connect an Ethernet port of the switch except the ninth port of ZXR10 2609/2809 to the network port of the background host by using a network cable. Check whether the connections are correct.
2. Restart the switch. At the HyperTerminal, press any key as prompted to enter the [ZxR10 Boot] state.

```
Welcome to use ZTE eCarrier!!


Copyright(c) 2004-2006,   ZTE Co.,  Ltd.
System Booting......
CPU: DB-88E6218
BSP version: 1.2/6-b
Creation date: Jan  3 2008,  11:46:44



Press any key to stop auto-boot...
 5

[ZXR10 Boot]:
```

3. Enter `c` in the **ZX10 Boot** state and press Enter to enter the parameter modification status. Set the IP addresses of the Ethernet port and the TFTP server. Generally, these two addresses are set to the same network segment.

```
[ZXR10 Boot]: c

'.' = clear field;  '-' = go to previous field;  ^D = quit

boot device          : marfec0        /*Use the default value*/
```

```
processor number     : 0              /*Use the default value*/
host name            : f129750        /*Use the default value*/
file name            : kernel         /*Use the default value*/
inet on ethernet (e) : 10.40.89.106   /*IP address of the Ethernet port*/
inet on backplane (b):                /*Use the default value*/
host inet (h)        : 10.40.89.78    /*IP address of the TFTP server*/
gateway inet (g)     : 10.40.89.78    /*Use the default value*/
user (u)             : 2952           /*Use the default value*/
ftp password (pw) (blank = use rsh): 2952 /*Use the default value*/
flags (f)            : 0x0            /*Use the default value*/
target name (tn)     :                /*Use the default value*/
startup script (s)   :                /*Use the default value*/
other (o)            : MAC0-00:32:45:67:89:ab /*Use the default value*/

Bootline has saved to NVRAM.
```

4. Set the IP address of the background host as the same with the IP address of the above TFTP server.
5. Start the TFTP server software on the background server and configure the TFTP by referring to TFTP configuration.
6. In the **ZX10 Boot** state, input **zte**, the screen prompts password should be entered, the default value is zxr10. After entering the password, enter the **BootManager** state of the switch. Input to display the command list for this state.

```
[ZxR10 Boot]: zte
[PASSWORD]:
Bootline has saved to NVRAM.

boot device          : marfec
unit number          : 0
processor number     : 0
host name            : f129750
file name            : kernel
inet on ethernet (e) : 10.40.89.106
host inet (h)        : 10.40.89.78
gateway inet (g)     : 10.40.89.78
user (u)             : 2952
ftp password (pw)    : 2952
flags (f)            : 0x0
other (o)            : MAC0-00:32:45:67:89:ab

Attached TCP/IP interface to marfec0.
Warning: no netmask specified.
Attaching network interface lo0... done.
Attaching to TFFS...
test flash passed perfectly!
Marvell has been initialized !
Welcome to boot manager!
Type '?' for help

[BootManager]: ?

ls
pwd
devs
show
reboot
format
setPassword
del    file_name
md     dir_name
mf     file_name
cd     absolute_pathname
tftp   ip_address file_name
upload ip_address file_name
update file_name
rename file_name  newname
[BootManager]:
```

7. In the **BootManager** state, use the command **tftp** to upgrade the version. The following shows how to download the version file from the TFTP server to the FLASH memory:

   TFTP command format: **tftp** <*ipaddress*><*filename*><*port-id*>, *port-id* is the port connecting the switch and TFTP host and can be connected to host by selecting any 100M port. Take port 8 as the example.

```
[BootManager]:tftp 10.40.89.78 kernel.z 8
Loading... done!
[BootManager]:ls
bootrom.bin              458768
snmpboots.v3                 35
startcfg.txt                682
running.cfg              539907
stacksystem.cfg             376
kernel.z                1572330
start.cfg                   364
[BootManager]:
```

8. In the **BootManager** state, execute the command **reboot** to restart the switch by using the new version. If the switch is started normally, use the command **show version** to check whether the new version is running in the memory. If the switch cannot be started normally, it indicates the version upgrade fails. In this case, repeat the above upgrade procedure from step 1.

Description about the Configuration File

Config.txt file is mainly used for version upgrade. When the span between new version and old one is big, using running.cfg file of the primary version may cause mistakes after version upgrade.

The correct operation steps are shown below.

1. Create config. txt file before implementing version upgrade.
2. Use the newly downloaded version to reboot switch after deleting running.cfg file of old version.

   Switch will use config.txt file to recover configurations. When command format is not modified or deleted in new version, the configurations will be recovered successfully.

   If configurations fails to recovery, recover them manually.
3. Use the command **saveconfig** to generate the new version running.cfg file after finishing the upgrade.

Chapter 7

Service Configuration

Table of Contents

Port Configuration....65
MAC Table Operations....71
Port Mirroring Configuration....73
Single Port Loop Detection Configuration....75
VLAN Configuration....78
GARP/GVRP Configuration....81
PVLAN Configuration....84
QinQ Configuration....86
SQinQ Configuration....89
LACP Configuration....91
STP Configuration....94
ZESR Configuration....102
IGMP Snooping Configuration....119
IPTV Configuration....124
DHCP CLIENT Configuration....131
DHCP Snooping/Option82 Configuration....133
VBAS Configuration....136
EPON....138
ACL Configuration....147
QoS Configuraton....156
Layer 2 Protocol Transparent Transmission Configuration....167
Layer 3 Configuration....169
Access Service Configuration....171
Syslog Configuration....182
NTP Configuration....183
OAM....185

Port Configuration

Port Overview

The commands can be classified into the following types to configure the port parameters.

1. Port basic parameters configuration
2. Port configuration about QoS
3. Port configuration about 802.1X

4. Port configuration about MAC
5. Configuration about multicast
6. Port information view

Port Basic Configuration

On ZXR10 2920/2928/2952/2936-FI, the port parameters such as auto negotiation, duplex mode and rate, flow control and MAC address number restriction and so on, can be configured

To configure the basic port parameters, perform the following steps.

Command	Function
zte(cfg)#**clear port** <*portlist*>{**name** | **statistics** | **description**}	This clears port name or statistics data.
zte(cfg)#**create port** <*portid*> **name** <*name*>	This creates port description name. **name** <*name*>: The port name can not be more than 200 characters. 1~255 is reserved, which can not be configured.
zte(cfg)#**set port** <*portlist*>{**enable** | **disable**}	This enables or disables the port. The port is disabled by default.
zte(cfg)#**set port** <*portlist*> **speedadvertise maxspeed**	This sets the port speedadvertise. Port speedadvertise is to set the negotiation speed between the local port and the other end port. If the gigabit port is set as speed100/fullduplex, the negotiation begins from the 100Mbps, fullduplex. When setting Maxspeed, the speed is 100Mbps, fullduplex for megabit port; the speed is 1000M, fullduplex for gigabit port.
zte(cfg)#**set port** <*portlist*> **speedadvertise maxspeed** {**speed10** | **speed100** | **speed1000**}{**fullduplex** | **halfduplex**}	
zte(cfg)#**set port** <*portlist*> **duplex** {**full** | **half**|**auto**}	This sets the working mode of port as fullduplex or halfduplex.
zte(cfg)#**set port** <*portlist*> **speed** {**10** | **100** | **1000**|**auto**}	This sets the speed of port as 10M/100Mbps/1000M.

Command	Function
zte(cfg)#**set port** <*portlist*> **default-priority** <*0-7*>	This sets the default priority of a port. It is a QoS related configuration command and used to specify the priority of untag packet received from this port. The default priority value is 0.
zte(cfg)#**set port**<*portlist*> **remapping-tag** <*0-7*> **priority** <*0-7*>	This sets 802.1P priority remapping on a port. This is a command relates to QoS. The port receives a packet with tag which includes priority setting information. The packet is mapped according to the setting information in the packet.
zte(cfg)#**set port** <*portlist*> **security** {**enable** | **disable**}	This enables or disables the security function on port. This function is used for access and authentication. Security function is disabled by default.
zte(cfg)#**set port** <*portlist*> **unit-statistics** {**enable** | **disable**}	This enables or disables the statistics function of port in unit time.
zte(cfg)#**set port** <*portlist*> **multicast-filter** {**enable** | **disable**}	This configures whether the port filters the multicast packet. It controls the forwarding of unknown multicast packet, mainly cooperating with the layer 2 multicast (IGMP Snooping/IPTV).
zte(cfg)#**set port** <*portid*> **description** <*string*>	This configures the description information of port. **<***string***>**: should be no more than 200 characters.
zte(cfg)#**set port** <*portlist*> **macaddress** {**on** <*1-100*>[**unkown-filter-en**]| **off**}	This sets the number of MAC address that the port can learn. The parameter unkown-filter-en is to control the forwarding of the unknown packet on the port.

Command	Function
zte(cfg)#**set port** <*port-list*> **mac-learning** {**enable** | **disable**}	This enables or disables port mac-learning. This controls MAC learning on port. The function is disabled by default. It learns and forwards the accessing packet on port.
zte(cfg)#**set port** <*portlist*> **acl** <*acl-number*>{**enable** | **disable**}	This configures the port bind with ACL rule.
zte(cfg)#**set port** <*portlist*>**vlanjump** {**enable** [**defaultauthvlan**<*1-4094*>]| **disable**}	This configures the VLAN that 802.1x unauthorization user can access. This function is mainly used with user accessing.
zte(cfg)#**set port** <*portlist*> **vlan-attrib ute** <*vlanlist*>{**untag** | **tag**}	This configures the corresponding configuration between port and vlan. The port and vlan has to be configured one to one.
zte(cfg)#**set queue-schedule feport** <*portlist*>{ **wrr0** | **wrr1-sp** | **wrr2-sp** | **sp**}	This sets the queue-schedule mode of 100Mbps port. This command relates to QoS and sets the queue-schedule mode on 100Mbps port. ▪ wrr0 queue-schedule mode 0 : WRRWRRWRRWRR ▪ SP queue-schedule mode 1 : SPSPSPSP ▪ WRR1-SP queue-schedule mode 2 : WRRWRRWRRSP ▪ WRR2-SP queue-schedule mode 3 : WRRWRRSPSP
zte(cfg)#**set queue-schedule geport** <*portlist*> **session** <*0,1*>	This sets the queue-schedule mode of gigabit port This command relates to QoS configuration.

Command	Function
zte(cfg)#**set port** <*portlist*> **user-priority** {**enable** | **disable**}	This configures the port trust 802.1p user priority. The default setting is enable.
zte(cfg)#**set port** <*portlist*> **dscp-priority** {**enable** | **disable**}	This sets the port trust IP DSCP priority. The default setting is disable.
zte(cfg)#**set sleep-mode** {**enable** | **disable**}	This enables or disables port sleep-mode. The default setting is disable.
zte(cfg)#**set jumbo geport** < *geportlist* >{ **enable** | **disable**}	This enables or disables jumbo frame on gigabit port. This controls the gigabit port forwarding of ultra-long packet. The default setting is disable.
zte(cfg)#**set jumbo feport** {**enable** | **disable**}	This enables or disables jumbo frame on 100Mbps port. This controls the forwarding of ultra-long packet on 100Mbps port. It takes effect on all 100Mbps ports. The default is disable.
zte(cfg)#**set port** <*portlist*> **accept-frame** {**tag** | **untag** | **all**}	This configures the frame type which can be received on port. By default, all types of frames are received. After receiving the specified type of frame, non-specified type of frame will be discarded.

When setting 100Mbps port trust DSCP, the switch also converts it to the corresponding UP (User priority). The flow is shown below.

When the IP message enters from port A that trusts in DSCP, firstly, get the default priority def[2:0](0-7, 3 bits in total) of port A. Then map the global DSCP-TC table according to DSCP value of the message, the initial TC value TC[1:0](0-3, 2 bits in total) of the message can be obtained. Adopt TC[1:0] as the [2:1]digit of UP and the last digit of port default priority def[0] as UP[0]digit of message. Therefore the new UP value UP[2:0] (0-7, 3 bits in total) is obtained. Finally, switch maps the global UP-TC table according to the new UP and get the queue that the message will enter.

The DSCP of a message is 60, the entry default priority is 7. DSCP is trusted. DSCP-TC mapping table is 60-2. Then in the switch, the UP message converts to 5, and obtain the queue to enter according to global UP-TC table.

Note:

When a port trusts UP and DSCP at the same time, the gigabit port will trust DSCP firstly, and the 100Mbps port will trust UP firstly.

Viewing Port Information

To view the port information, perform the following steps.

Command	Function
zte(cfg)#**show port** [<*portlist*>]	This displays the configuration and work state of the port.
zte(cfg)#**show port** <*portlist*> **vlan**	This displays Vlan information of the port.
zte(cfg)#**show port** <*portlist*> **statistics** [**1min_unit** | **5min_unit**]	This displays statistics information of the port.
zte(cfg)#**show port** <*portlist*> **utilization**	This displays utilization statistics of the port.
zte(cfg)#**show port** <*portlist*> **qos**	This displays the QoS configuration on a port.
zte(cfg)#**show port** <*portlist*> **bandwidth session** <*0-3*>	This displays the bandwidth information on a port.
zte(cfg)#**show port** <*portlist*> **brief**	This displays the brief information of a port.

One end is auto-negotiation port. Another end is forced rate port. The joint result is shown below.

Auto-negotiation port	Forced rate port				
	10M Full	10M Half	100M Full	100M Half	1000M Full
100M auto	10M Half	10M Half	100M Half	100M Half	joint un-success-fully
1000M auto	10M Half	10M Half	100M Half	100M Half	1000M Full

MAC Table Operations

MAC Table Overview

MAC table operations include the configuration of MAC filter function, static address binding function and MAC table aging time.

- MAC filter function is to enable the switch to discard the received data packets whose source or destination MAC address is the specified MAC address.
- Static address binding function is to bind the specified MAC address with the switch port. After the binding, this MAC can't be the dynamically learned any more.
- MAC table aging time refers to the period from the latest update of dynamic MAC address in the FDB table to the deletion of this address.

Configuration of the MAC filter function and static address binding function can effectively prevent the illegal access to the network and fraudulent use of key MAC addresses, and play an important role in ensuring the network security.

Basic Configuration of MAC Table

To configure FDB, perform the following steps.

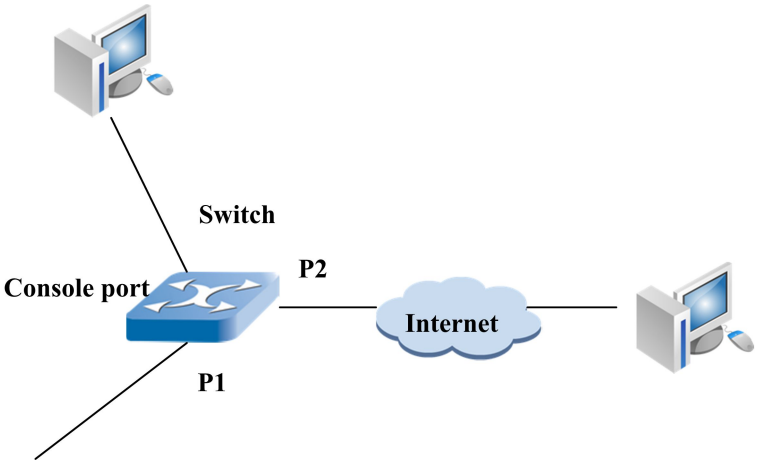
Command	Function
`zte(cfg)#`**set fdb add** *<HH.HH.HH.HH.HH.HH>* **vlan** *<1-4094>*{**port** *<portid>*| **trunk** *<trunkid>*}	This adds the static binding address to the address table.
`zte(cfg)#`**set fdb agingtime** *<40-1260>*	This sets the aging time of MAC address. The parameter **agingtime** is 240 seconds by default.
`zte(cfg)#`**set fdb delete** *<HH.HH.HH.HH.HH.HH >* **vlan** *<1-4094>*	This deletes a record from MAC address table.
`zte(cfg)#`**set fdb filter** *<HH.HH.HH.HH.HH.HH vlan <1-4094>*	This sets the filter address of fdb.
`zte(cfg)#`**show fdb** [**static** | **dynamic** | **filter**][**detail**]	This displays fdb information.
`zte(cfg)#`**show fdb agingtime**	This displays the aging time of fdb.

Command	Function
zte(cfg)#**show fdb mac** <*HH.HH.HH.HH.HH.HH*>	This displays the fdb information of MAC address.
zte(cfg)#**show fdb port** <*portid*>[**detail**]	This displays the fdb information of a port.
zte(cfg)#**show fdb trunk** <*trukid*>[**detail**]	This displays the fdb information of a Trunk group.
zte(cfg)#**show fdb vlan** <*vlanid*>[**detail**]	This displays the fdb information of a VLAN.

FDB Configuration Example

As shown in Figure 39, this sets MAC address table management through console port. Set the dynamic MAC aging time to 300S . Bind a static MAC 00.D0.D0.29.20.92 in port 2 of VLAN 1. The maximum number of access user of port 1 is 100. Forbid device with MAC 00.D0.D0.00.00.01 access to the network.

FIGURE 39 FDB CONFIGURATION EXAMPLE



Configuration of switch:

1. Configuration procedure:

```
zte(cfg)#set fdb agingtime 300
zte(cfg)#set fdb add 00.d0.d0.29.20.92 vlan 1 port 2
zte(cfg)#set fdb filter 00.d0.d0.00.00.01 vlan1
zte(cfg)#set port 1 macaddress on 100
```

2. Configuration check:

   i. This following example describes how to show the total MAC address table.

```
zte(cfg)#show fdb detail
  MacAddress       Vlan  PortId    Type
  -----------------      -----  --------   --------
  00.00.00.00.00.01    1     1       dynamic
00.00.00.00.00.0b   1      1       dynamic
```

```
00.00.00.00.00.15   1     1       dynamic
00.00.00.00.00.29   1     1      dynamic
/*access to network user MAC*/
00.d0.d0.00.00.01   1     -        filter
/*forbid this MAC access to network*/
00.d0.d0.29.20.92   1     2        static
/*bind the static MAC in VLAN 1 to port 2*/
Total: 7
```

ii. This following example shows how to view the maximum number of access user on port 1.

```
zte(cfg)#show port 1
  PortId     : 1               MediaType : 100BaseT
  PortParams:
    PortEnable     : enabled       PortAutoNeg    : enabled
    DefaultVlanId  : 1             FlowControl    : disabled
    Multicastfilter: disabled          Security       : disabled
    SpeedAdvertise : MaxSpeed      Mdix           : auto
    PortMacLimit   : 100           UnknownFilter  : disabled
    MacLearning    : enabled
    PortVlanJump   : disabled
  PortStatus:
    PortClass      : 802.3         Link           : up
Duplex         : full          Speed          : 100Mbps
```

Through **show port** command, PortMacLimit shows the maximum number of port learning MAC address, that is, the number of port permitting user to access.

Port Mirroring Configuration

Port Mirroring Overview

Port mirroring is used to mirror data packets of the switch port (ingress mirroring port) to an ingress destination port (ingress monitoring port), or mirror the data packets of the switch port (egress mirroring port) to an egress destination port (egress monitoring port).

By using mirroring, data packets flowing in or out of a certain port can be monitored. Port mirroring provides an effective tool for the maintenance and monitoring of the switch.

Switch can be configured with only one ingress monitoring port and one egress monitoring port. Ingress monitoring port and egress monitoring port can be configured on the same port. Whereas multiple source ingress monitoring ports and source egress monitoring ports can be configured at the same time.

Note:

In default case, switch does not have mirroring port or monitoring port. The correct data packets received by ingress mirroring port are mirrored onto the monitoring ports, but data packets directly discarded on the ingress port (for example, because of CRC errors) are not mirrored.

Port Mirroring Basic Configuration

To mirror the ports, perform the following steps.

Command	Function
zte(cfg)#**set mirror add source-port** <*portlist*>{**ingress** | **egress**}	This adds an egress or ingress mirroring port.
zte(cfg)#**set mirror delete source-port** <*portlist*>{**ingress** | **egress**}	This deletes an egress or ingress mirroring port.
zte(cfg)#**set mirror add dest-port** <*portid*>{**ingress** | **egress**}	This sets an egress or ingress monitoring port.
zte(cfg)#**set mirror delete dest-port** <*portid*>{**ingress** | **egress**}	This deletes an egress or ingress monitoring port.
zte(cfg)#**set mirror statistic** {**ingress** | **egress**} **sample-interval** <*1-2047*>	This sets sample mirror statistic rate.
zte(cfg)#**show mirror**	This displays the configuration information of port mirroring.

Example

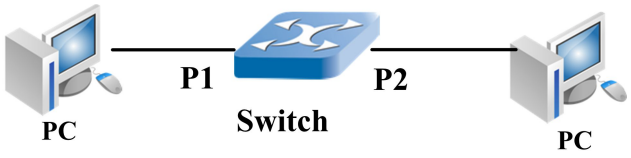
```
zte(cfg)#show mirror
  Ingress mirror information:
  ---------------------------
    Ingress statistical mirror :    sample-interval 1
    Source port: none
    Destination port: none

  Egress mirror information:
  ---------------------------
    Geport(sub card) egress statistical mirror :     sample-interval 1
    Source port: none
    Destination port: none
```

Port Mirroring Configuration Example

This example describes how to configure port mirroring on switch and port 2 can monitor the packets on port 1, as shown in Figure 40.

FIGURE 40 PORT MIRRORING CONFIGURATION EXAMPLE



The configuration of switch:

1. The following example describes how to set port mirroring on ingress direction.

```
zte(cfg)#set mirror add source-port 1 ingress
zte(cfg)#set mirror add dest-port 2 ingress
zte(cfg)#set mirror statistic ingress sample-interval 100
/*set the port sample-interval of mirror statistic */
```

2. The following example describes how to set port mirroring on egress direction.

```
zte(cfg)#set mirror add source-port 1 egress
zte(cfg)#set mirror add dest-port 2 egress
zte(cfg)#set mirror statistic egress sample-interval 100
```

Note:

For the port mirroring on egress direction, the mirroring destination port has to be a gigabit port or be a subcard port. Otherwise, the normal port mirroring will be implemented.

3. The following example describes how to view port mirroring.

```
zte(cfg)#show mirror
  Ingress mirror information:
  ---------------------------
    Ingress statistical mirror :    sample-interval 100
/*if sample interval is 1, then it is normal port mirroring. */
    Source port: 1
    Destination port: 2

  Egress mirror information:
  --------------------------
Geport(sub card) egress statistical mirror :     sample-interval 100
/*If sample interval=1 or mirroring destination port is not gigabit
port or daughter card port, then normal port mirroring is done.*/
    Source port: 1
    Destination port: 2
```

Single Port Loop Detection Configuration

Loop Detection Overview

Single port loop detection is to check whether a loop exists in the ports of the switch. If such a loop exists, it may result in errors in learning MAC addresses and may easily cause a broadcast storm. In severe case, switch and network may be down. Starting the single port loop detection and disabling the port with loop can efficiently avoid the influence caused by port loop.

The switch sends a test packet through a port. If this test packet is received through the port without any change (or only a tag is attached), it indicates that a loop exists in this port.

The test packet sent by the switch includes the following three parameters:

- Source MAC address: It indicates the MAC address of the switch. The MAC address of each switch is unique.
- Port Number: Port numbers correspond to the numbers of the ports on the switch one by one.
- Discrimination Field: For each switch, the digital signature of each port is different.

When three parameters in the receiving and sending test packets are same, the loop definitely exists on this port.

Configuring Single Port Loop Detection

To configure single port loop detection, perform the following steps.

Command	Function
zte(cfg)#**set loopdetect port** <*portlist*>{**enable** | **disable**}	This enables or disables loop test function on a specified port. When the VLAN is not specified to examine, examine the VLAN where the port PVID exists. By default, port loop detection function is disabled.
zte(cfg)#**set loopdetect port** <*portlist*> **vlan** <*1-4094*>	This enables or disables loop detection function of specified port in specified vlan. By default, port loop detection function is disabled.
zte(cfg)#**set loopdetect trunk** <*trunklist*>{**enable** | **disable**}	This enables or disables loop detection function of a trunk. This command examines the Vlan where the trunk PVID exists. By default, loop detection function of a trunk is disabled.
zte(cfg)#**set loopdetect trunk** <*trunklist*> **vlan** <*1-4094*>	This enables or disables loop detection function of a trunk on a vlan. By default, loop detection function of a trunk is disabled.

Command	Function
zte(cfg)#**set loopdetect trunk** <*trunklist*> **protect** {**enable** | **disable**}	This enables or disables loop detection protection function on a specified port. Loop detection protection function means that port is automatically blocked to reduce the influence on port loop when it detects a loop.
zte(cfg)#**set loopdetect blockdelay** <*1-1080*>	This sets time for blocking port with loop. Time for blocking port with loop refers to time for blocking port when a loop is detected, that is, port protection time. Protection takes effect only when loop detection protection function of port is enabled.
zte(cfg)#**set loopdetect sendpktinterval** <*5-60*>	This sets interval time for sending loop detection packet. Loop detection function sends test packet on time, and judges whether there is a self-loop by judging whether the packet is received in the interval time. The default value is 15 seconds.
zte(cfg)#**set loopdetect extend port** <*portlist*>{**enable** | **disable**}	This sets cross-devices loop detection. This command implements cross-devices port loop detection on ZXR10 Ethernet switch. Disable STP function on port before enabling function. Enable single port loop detection on the related port before enabling this function. This function is disabled by default.
zte(cfg)#**show loopdetect**	This displays port loop detection configuration and port detection status.

When the port can not work normally, use the command show loopdetect to observe whether a port loop exists. If no loop is

detected and the spanning tree of the port is enabled, eliminate fault according to status of spanning status, as shown below.

```
The block-delay interval of loopback detection is 5 minutes.
The send loopdetect packet interval of loopback detection is 15 seconds.
PortId Stp Trunk Link Loop Protect VlanId Status Extend
------ ---- ----- ----- ----- ------- ------- ------
 29 No No Up N/A Yes default N/A No
 30 No No Up N/A Yes default N/A No
 31 No No Up N/A Yes default N/A No
 32 No No Up N/A Yes default N/A No
```

The description of parameters is shown below.

PortId: The port which enables loop detection function.

Stp: Whether the port is STP port or not.

Trunk: Whether the port is link aggregation port or not.

Link: The current state of port.

Loop: Whether the loop exists on link or not.

Protect: Whether the loop protection function is enabled on this port.

VlanId: The VLANs which are permitted to use loop detection function.

VLAN Configuration

VLAN Overview

The Virtual Local Area Network (VLAN) protocol is a basic protocol of layer 2 switching equipment, which enables the administrator to divide a physical LAN to multiple VLANs. Each VLAN has a VLAN ID to identify it uniquely in the entire LAN. Multiple VLANs share the switching equipment and links of the physical LAN.

Logically, a VLAN is like an independent LAN. All frame flows in the same VALN are restricted in this VLAN. Cross-VLAN visit can only be implemented through forwarding on layer 3. In this way, the network performance is improved, and the overall flow in the physical LAN is effectively lowered.

The VLAN has the following functions:

1. Reduce the broadcast storms of network.
2. Enhance the network security.
3. Provide centralized management and control.

The ZXR10 2920/2928/2952/2936-FI also supports the tagged-based VLAN. This is a mode defined in IEEE 802.1Q and also is a universal working mode. In this mode, the division of VLAN is based on the VLAN information about the port (PVID: port VLAN ID) or the information in the VLAN tag.

Basic Configuration of VLAN

The VLAN configuration on the switch includes the following contents:

Command	Function
zte(cfg)#**clear vlan** <*vlanlist*> **name**	This removes a VLAN name.
zte(cfg)#**create vlan** <*14094*> **name** <*name*>	This creates a VLAN description name. **<***string***>**: The name of VLAN can not be only a number , and should be less than 64 characters.
zte(cfg)#**set port** <*portlist*> **pvid** <*14094*>	This sets PVID on port.
zte(cfg)#**set trunk** < *trunklist* > **pvid** <*14094*>	This sets PVID of trunk.
zte(cfg)#**set vlan** <*vlanlist*>{**enable**|**disable**}	This enables or disables VLAN. By default, VLAN 1 is enabled, other VLANs are disabled.
zte(cfg)#**set vlan** <*vlanlist*> **add port** <*portlist*>[**tag**|**untag**]	This adds a specified port to VLAN.
zte(cfg)#**set vlan** <*vlanlist*> **delete port** <*portlist*>	This deletes a specified port from VLAN.
zte(cfg)#**set vlan** <*vlanlist*> **add trunk** <*trunklist*>[**tag**|**untag**]	This adds a specified trunk to VLAN.
zte(cfg)#**set vlan** <*vlanlist*> **delete trunk** <*trunklist*>	This deletes a specified trunk from VLAN.
zte(cfg)#**set vlan** <*vlanlist*> **forbid port** <*portlist*>	This forbids learning port on VLAN. It is mainly used with GVRP.
zte(cfg)#**set vlan** <*vlanlist*> **permit port** <*portlist*>	This permits learning port on VLAN. It is mainly used with GVRP.
zte(cfg)#**set vlan** <*vlanlist*> **forbid trunk** <*trunklist*>	This forbids learning trunk on VLAN. It is mainly used with GVRP.
zte(cfg)#**set vlan** <*vlanlist*> **permit trunk** <*trunklist*>	This permits learning trunk on VLAN. It is mainly used with GVRP.

Command	Function
zte(cfg)#**set vlan-translation ingress-port** <*feport-id*>{ **enable** | **disable** }	This enables or disables VLAN translation.
zte(cfg)#**clear vlan-translation ingress-port** <*feport-id*>	This clears the configuration of VLAN translation.
zte(cfg)#**set vlan-translation ingress-port** <*feport-id*> **ingress-vlan** <*vlan-list*> **egress-port** <*geport-id*> **egress-vlan** <*vlan-list*>	This sets VLAN translation.
zte(cfg)#**show vlan** [<*vlanlist*>]	This displays VLAN information.

Note:

The logic link through link aggregation is called as Trunk. One Trunk is composed of multiple physical ports. Refer to "Basic Configuration of LACP" for more detailed information.

VLAN Configuration Example

1. The following example shows how to configures a VLAN.

   Note:

   By default, VLAN1 is enabled, all ports are in VLAN1 and in mode of untag.

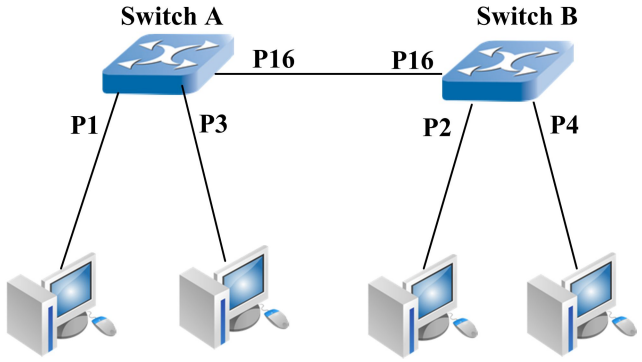
   Configure VLAN 100. Add untagged ports 1 and 2 and tagged ports 7 and 8. The detailed configuration is as follows:

```
zte(cfg)#set vlan 100 add port 1, 2 untag
zte(cfg)#set vlan 100 add port 7, 8 tag
zte(cfg)#set port 1, 2 pvid 100
zte(cfg)#set vlan 100 enable
zte(cfg)#show vlan 100
  VlanId  : 100   VlanStatus: enabled
  VlanName:
  VlanMode:     Static
  Tagged ports  : 7-8
  Untagged ports: 1-2
  Forbidden ports:
```

2. The following example shows how to configure the VLAN transparent transmission.

   As shown in Figure 41, switch A is connected to switch B through port 16. Port 1 of switch A and port 2 of switch B belong to VLAN2, and port 3 of switch A and port 4 of switch B belong to VLAN3. Members of the same VLAN can communicate with each other.

FIGURE 41 EXAMPLE OF VLAN TRANSPARENT TRANSMISSION



The detailed configuration on the switch A is as follows:

```
zte(cfg)#set vlan 2 add port 16 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add port 16 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

The detailed configuration on the switch B is as follows:

```
zte(cfg)#set vlan 2 add port 16 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add port 16 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

GARP/GVRP Configuration

GARP/GVRP Overview

GARP is a kind of generic attribute registration protocol, which distributes VLAN and multicast MAC address dynamically to the member in the same switching network by applying the different application protocols.

GVRPGARP VLAN Registration Protocolis a kind of application protocol defined by GARP, which maintains VLAN information in switch dynamically based on GARP protocol mechanism. All switches supporting GVRP can receive the VLAN registration information from other switches and update local VLAN registration information dynamically including the current VLAN on this switch and the ports in this VLAN. Also all switches supporting GVRP can broadcast the local VLAN registration information to other switches, so that, the VLAN configurations of all devices with GVRP in the same switching network have the consistent interworking according to demand.

Configuring GARP/GVRP

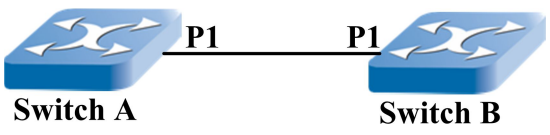
The GARP/GVRP configuration covers the following contents.

Command	Function
zte(cfg)#**set garp** {**enable** | **disable**}	This enables or disables GARP function. By default GARP is disabled.
zte(cfg)#**set garp timer**{**hold**|**join**|**leave**|**leaveall**}<*timer_value*>	This sets GARP timer.The parameter **<***timer_value***>** takes the fixed value 100.
zte(cfg)#**show garp**	This shows the configuration of GARP.
zte(cfg)#**set gvrp** {**enable** | **disable**}	This enables or disables GVRP function.
zte(cfg)#**set gvrp port** <*portlist*>{**enable**|**disable**}	This enables or disables GVRP function on port.
zte(cfg)#**set gvrp port** <*portlist*> **registration**{**normal**|**fixed**|**forbidden**}	This configures type of GVRP registration on port.
zte(cfg)#**set gvrp trunk** <*trunklist*>{**enable**|**disable**}	This enables or disables GVRP on trunk port.
zte(cfg)#**set gvrp trunk**<*trunklist*> **registration**{**normal**|**fixed**|**forbidden**}	This configures GVRP registration type on Trunk port.
zte(cfg)#**show gvrp**	This views GVRP configuration information including if GVRP can be enabled and GVRP configuration status of each port and each Trunk port.

GARP/GVRP Configuration Example

As shown in Figure 42, switch A connects with switch B through port 1. By configuring GVRP, the two switches can register each other and refresh their VLAN table.

FIGURE 42 GVRP CONFIGURATION EXAMPLE



Configuration of switch A:

```
zte(cfg)#set garp en
zte(cfg)#set gvrp en
zte(cfg)#set gvrp port 1 en
zte(cfg)#set vlan 10-20 en
zte(cfg)#set vlan 10-20 add port 1
```

Configuration of switch B:

```
zte(cfg)#set garp en
zte(cfg)#set gvrp en
zte(cfg)#set gvrp port 1 en
zte(cfg)#set vlan 30-40 en
zte(cfg)#set vlan 30-40 add port 1
```

Configuration check:

```
SwitchA(cfg)#show garp  /*View GARP configuration*/
GARP is enabled!
  GARP Timers:
  Hold Timeout      :100 milliseconds
  Join Timeout      :200 milliseconds
  Leave Timeout     :600 milliseconds
LeaveAll Timeout  :10000 milliseconds

SwitchA(cfg)#show gvrp  /*View GVRP configuration*/
GVRP is enabled!
  PortId   Status   Registration     LastPduOrigin
  ------    --------  ------------     -----------------
  1      Enabled   Normal     00.d0.d0.f2.51.24
SwitchA(cfg)#show port 1 vlan
  PortId  : 1
Tagged in vlan   : 30-40
Untagged in vlan : 1, 10-20
SwitchB(cfg)#show port 1 vlan
  PortId  : 1
  Tagged in vlan   : 10-20
Untagged in vlan : 1, 30-40
SwitchA(cfg)#show vlan 30-40
VlanId  : 30     VlanStatus: enabled
  VlanName:
  VlanMode: Dynamic
  Tagged ports    :  1
  Untagged ports  :
  Forbidden ports :
SwitchB(cfg)#show vlan 10-20
VlanId  : 10    VlanStatus: enabled
  VlanName:
  VlanMode: Dynamic
  Tagged ports    :1
  Untagged ports  :
  Forbidden ports :
```

Caution:

1. Garp function should be enabled first before Gvrp function is enabled.
2. Enabling GVRP can enable up to 256 vlans.
3. Timer of Garp generally uses the default value. If it is modified, the value must be the same as the one configured in the network.
4. Gvrp port registration type uses default Normal value. If it is modified to other types, vlan learning can’t be done.

PVLAN Configuration

PVLAN Overview

PVLAN (Private VLAN) is a port-based VLAN. It consists of many promiscuous ports and isolated ports. Isolated ports can not access each other, but isolated ports and promiscuous ports can access each other.

ZXR10 2920/2928/2952/2936-FI supports 4 PVLANs. Each PVLAN supports a promiscuous port. There is no restriction for isolated ports number, but they can not be gigabit ports.

PVLAN permits the user to access server, but the direct inter-access between users is not permitted. Therefore, the configuration only takes effect on a whole PVLAN area (the shared and isolated ports exist together). The promiscuous and isolated ports are necessary to be configured, otherwise, the configuration of PVLAN will be invalid.

Basic Configuration of PVLAN

To configure PVLAN, perform the following steps.

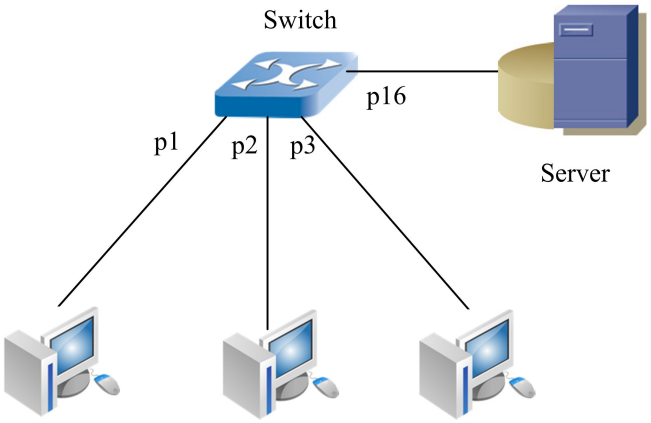
Command	Function
zte(cfg)#**set pvlan session** <*1-4*> **add promiscuous** {**port**<*portid*>|**trunk**<*trunkid*>} **isolate-port** <*portlist*>	This adds the isolate ports and promiscuous ports into PVLAN instance.
zte(cfg)#**set pvlan session** <*1-4*> **delete isolate-port** <*portlist*>	This deletes the isolate ports from PVLAN instance. When only one isolated port exists, this port can not be deleted.
zte(cfg)#**set pvlan session** <*1-4*> **modify promiscuous** {**port** <*portid*>| **trunk** <*trunkid*>}	This modifies the uplink port in PVLAN instance.
zte(cfg)#**set pvlan session** <*1-4*> **clear-config**	This clears PVLAN session configuration.
zte(cfg)#**show pvlan**	This views PVLAN configuration.

PVLAN Configuration Example

1. Example 1

As shown in Figure 43, add promiscuous port 16 and isolated ports 1, 2, and 3 to session 1.

FIGURE 43 PVLAN CONFIGURATION EXAMPLE 1



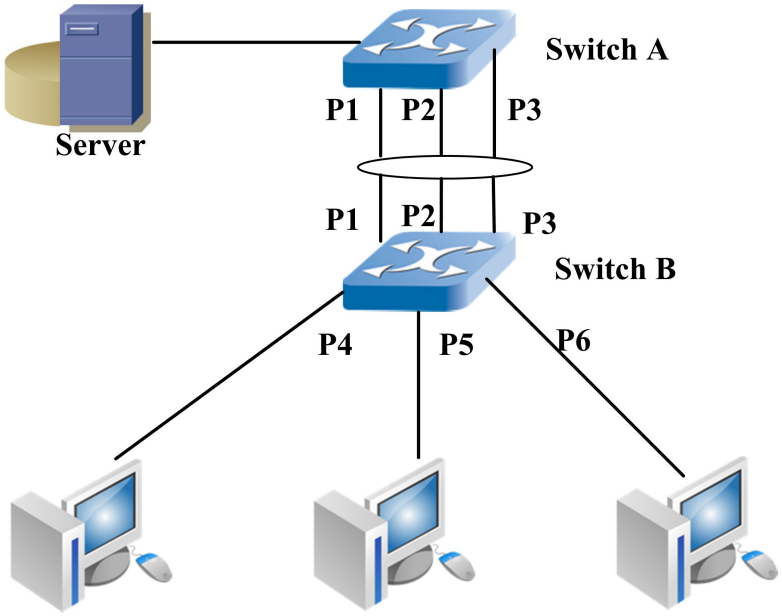
The detailed configuration of switch is as follows:

```
zte(cfg)#set pvlan session 1 add promiscuous
 port 16 isolate-port 1-3
zte(cfg)#show pvlan
pvlan session    : 1
  promiscuous-port: 16
  isolated-port    : 1-3
```

2. Example 2

As shown in Figure 44, add trunk 1 and isolated port 4, 5 and 6 into session 2.

FIGURE 44 PVLAN CONFIGURATION EXAMPLE 2



Configuration of switch A:

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 1 add port 1-3
zte(cfg)#set lacp sggregator 1 mode dynamic
```

Configuration of switch B:

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 1 add port 1-3
zte(cfg)#set lacp aggregator 1 mode dynamic
zte(cfg)#set pvlan session 2 add promiscuous trunk 1 isolate-port 4-6
zte(cfg)# zte(cfg)#show pvlan
  pvlan session    : 1
  promiscuous-port:
  isolated-port    :

  pvlan session    : 2
  promiscuous-port: T1
  isolated-port    : 4-6
```

Note:

The promiscuous port can be Trunk, but the isolated port can not be Trunk.

QinQ Configuration

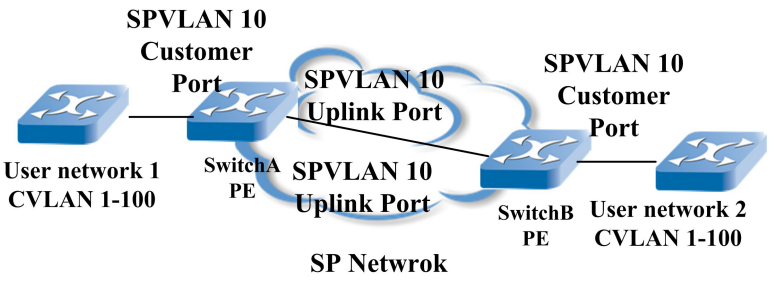
QinQ Overview

QinQ is the IEEE 802.1Q tunneling protocol and is also called VLAN stacking. QinQ technology is the addition of one more VLAN tag (outer tag) to the original VLAN tag (inner tag). The outer tag can shield the inner tag.

QinQ does not need the protocol support. The simple Layer 2 Virtual Private Network (L2VPN) can be realized through QinQ. The QinQ is especially suitable for the small-size LAN that takes the layer 3 switch as its backbone.

Figure 45 shows the typical networking of the QinQ technology. The port connected to the user network is called Customer port. The port connected to the ISP network is called Uplink port. The edge access equipment of the ISP network is called Provider Edge (PE).

FIGURE 45 TYPICAL QINQ NETWORKING



1. SPVLAN Service Provider VLAN
2. CVLAN Customer VLAN

The user network is generally connected to the PE through the Trunk VLAN mode. The internal Uplink ports of the ISP network are symmetrically connected through the Trunk VLAN mode.

1. When a packet is sent form user network 1 to the customer port of switch A, because the PORTBASE VLAN-based customer port does not identify the tag when receiving the packet, the customer port processes the packet as an untagged packet no matter whether this data packet is attached with the VLAN tag or not. The packet is forwarded by the VLAN 10, which is determined by the PVID.
2. The uplink port of switch A inserts the outer tag (VLAN ID: 10) when forwarding the data packet received from the customer port. The tpid of this tag can be configured on the switch. Inside the ISP network, the packet is broadcast along the port of VLAN 10 until it reaches the switch B.
3. Switch B finds out that the port connected to user network 2 is a customer port. Thus, it removes the outer tag in compliance with the conventional 802.1Q protocol to recover the original packet and sends the packet to user network 2.
4. In this way, data between user network 1 and user network 2 can be transmitted transparently. The VLAN ID of the user network can be planned regardless of the conflict with the VLAN ID in the ISP network.

Basic Configuration of QinQ

The QinQ configuration on the switch includes the following contents:

Command	Function
`zte(cfg)#` **set qinq customer port** <*portlist*>{**enable**|**disable**}	This adds/deletes a Customer port.
`zte(cfg)#` **set qinq uplink port** <*portlist*>{**enable**|**disable**}	This adds/deletes an Uplink port.
`zte(cfg)#` **set qinq tpid** <*tpid*>	This sets the tpid of the outer tag.
`zte(cfg)#` **show qinq**	This displays the QinQ configuration.

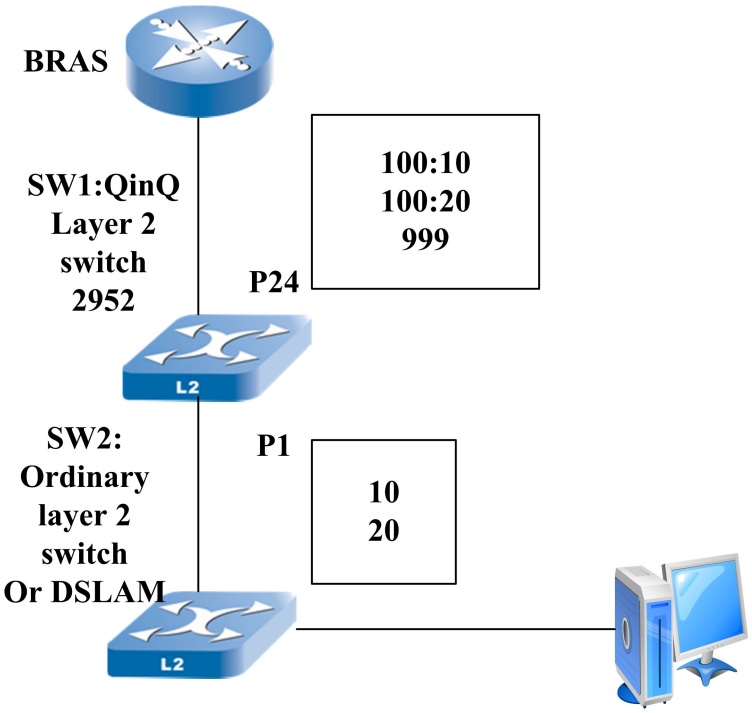
Note:

When the QinQ is configured, the customer port and the uplink port of SPVLAN can be set as an untagged port or as a tagged port.

QinQ Configuration Example

As shown in Figure 46, encapsulate an exterior label in SW1 (ZXR10 2952) for the packet from SW2. The VLAN number is 100. The port connecting upstream BRAS in SW1 is port 24. The port connecting downstream SW2 is port 1. The NM vlan of SW1 is 999 and the management IP address is 192.168.0.1/24.

FIGURE 46 QINQ CONFIGURATION EXAMPLE



Configuration of switch:

Configuration on SW1(ZXR10 2952):

```
/* set qinq, the outer label is 100*/
zte(cfg)#set vlan 100 enable
zte(cfg)#set vlan 100 add port 1, 24
 zte(cfg)#set port 1, 24 pvid 100
zte(cfg)#set qinq customer port 1 enable
zte(cfg)#set qinq uplink port 24 enable
zte(cfg)#set vlan 999 enable
zte(cfg)#config router
zte(cfg-router)#set ipport 1 ipaddress 192.168.0.1/24
zte(cfg-router)#set ipport 1 vlan 999
zte(cfg-router)#set ipport 1 enable
zte(cfg-router)#exit
```

SQinQ Configuration

SQinQ Overview

SQinQ (Selective QinQ) is based on QinQ technology and is the abbreviation of Selective QinQ. Compared to ordinary QinQ, it enables packets to be tagged with outer tags according to inner tag.

SQinQ uses same terms as QinQ to describe its features: Port connected to Client Network is called Customer port. Port connected to Service Provider Network is called Uplink port. Accessing equipment at the edge of Service Provider Network is called PE (Provider Edge). Client Network is accessed to PE via Trunk VLAN. Uplink Ports inside Service Provider Network are connected via Trunk VLAN symmetrically. SQinQ is based on ACL function. By matching specific ACL traffic rules in ports, SQinQ functions can set different Service Provider's VLAN tags for packets. Packets are transmitted in Service Provider Network. Vlan Tags of Service Provider would be strip off when packets leave Service Provider Vlan.

SQinQ configuration includes the following two steps:

1. Customer Port Strategy Configuration

   Configure a group of customer vlans corresponding to one uplink vlan. One port can configure multiple customer vlan groups, but must make sure that vlan can't overlap in different customer vlan groups on the same port.

   Configuration of SQinQ in CustomerPort only makes sense for packets which carrying 802.1Q tag and for designated Customer Vlan. As to the Customer Vlan which carries 802.1P tag or untag, It are all handled as normal Vlan.

   Note:

   SQinQ would not work in good condition when QinQ is already configured. Reason is that port could not recognize Customer Vlan Tag any more when QinQ is configured on this port. Consequently, SQinQ would not get any Customer Vlan information.

2. ISP vlan Configuration

   It is necessary to operate Service Provider Network after CustomerPort configuration. Packets can be exchanged successfully. Configure all ports in Service Provider Network as Tag Ports and all Customer Ports as Untag Ports. All the packets exchanged in Service Provider Network carry two layers of Tag which are Uplink Tag and Customer Tag. When packets leaving Service Provider Network, there is only one layer of Tag left: Customer Tag.

Basic Configuration of SQinQ

To configure SQinQ, perform the following steps.

Command	Function
zte(cfg)#**set sqinq-session** <*1-256*> **customer-vlan** <*vlanlist*> **uplink-vlan** <*1-4094*>	This configures SQinQ session.
zte(cfg)#**set policy policing in sqinq-session** <*1-256*> **policer** <*0-255*>	This configures traffic rate limitation.
zte(cfg)#**clear policy policing in sqinq-session** <*1-256*>	This clears traffic rate limitation.
zte(cfg)#**set policy statistics in sqinq-session** <*1-256*> **counter** <*0-31*>	This configures traffic statistics.
zte(cfg)#**clear policy statistics in sqinq-session** <*1-256*>	This clears traffic statistics.
zte(cfg)#**set policy mirror in sqinq-session** <*1-256*> **analyze-port**	This sets traffic mirror.
zte(cfg)#**clear policy mirror in sqinq-session** <*1-256*>	This clears traffic mirror.
zte(cfg)#**set port** <*portlist*> **sqinq-session** <*sessionlist*>{**enable** | **disable**}	This applies SQinQ session on port.
zte(cfg)#**clear sqinq-session** <*sessionlist*>	This clears the configuration of SQinQ session.
zte(cfg)#**show sqinq-session** [<*sessionlist*>]	This shows SQinQ session.

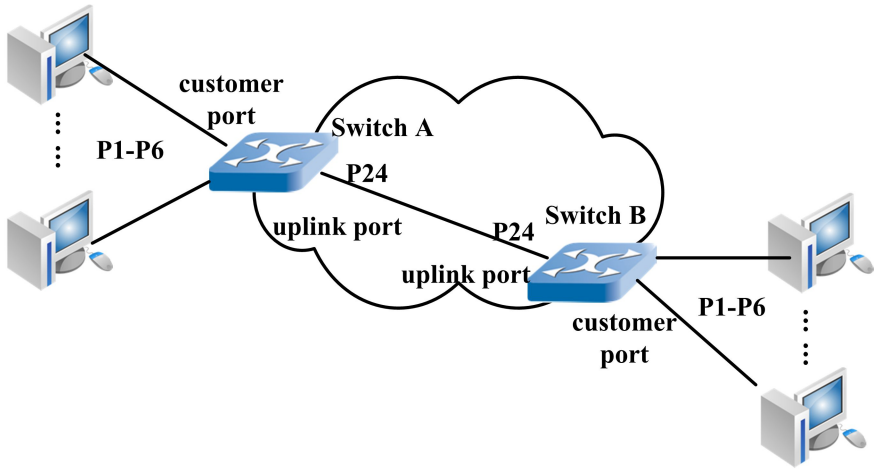
Note:

When configuring SQinQ, policy configuration of SQinQ refers to the related description about QoS.

SQinQ Configuration Example

As shown in Figure 47, there are two switches of ZXR10-2952 (Switch A and Switch B) in Service Provider Network. Port 24 of Switch A is connected to port 24 of Switch B. Vlan1-200 is in port 1–6 of Switch A which communicate with port 1–3 of Switch B in which Uplink vlanid assigned as 100. Vlan201-4094 is in port 1–6 of Switch A which communicates with port 4–6 of Switch B in which Uplink vlanid assigned as 200. CustomerPort of Switch A is untag port only for Vlan1.

FIGURE 47 SQINQ TYPICAL NETWORK



Configuration of switch A:

```
zte(cfg)#set sqinq-session 1 customer-vlan 1-200 uplink-vlan 100
zte(cfg)#set vlan 100 enable
zte(cfg)#set port 1-6 sqinq-session 1 enable
zte(cfg)#set vlan 100 add port 1-6 untag
zte(cfg)#set vlan 100 add port 24 tag
zte(cfg)#set port 1-6 pvid 100
zte(cfg)#set sqinq-session 2 customer-vlan 201-4094 uplink-vlan 200
zte(cfg)#set vlan 200 enable
zte(cfg)#set port 1-6 sqinq-session 2 enable
zte(cfg)#set vlan 200 add port 4-6 untag
zte(cfg)#set vlan 200 add port 24 tag
```

Configuration of switch B:

```
zte(cfg)#set sqinq-session 1 customer-vlan 1-200 uplink-vlan 100
zte(cfg)#set vlan 100 enable
zte(cfg)#set port 1-3 sqinq-session 1 enable
zte(cfg)#set vlan 100 add port 1-3 untag
zte(cfg)#set vlan 100 add port 24 tag
zte(cfg)#set port 1-3 pvid 100
zte(cfg)#set sqinq-session 2 customer-vlan 201-4094 uplink-vlan 200
zte(cfg)#set vlan 200 enable
zte(cfg)#set port 4-6 sqinq-session 2 enable
zte(cfg)#set vlan 200 add port 4-6 untag
zte(cfg)#set port 4-6 pvid 200
zte(cfg)#set vlan 200 add port 24 tag
```

LACP Configuration

LACP Overview

Link Aggregation Control Protocol (LACP) is a standard protocol defined in IEEE 802.3ad.

Link aggregation means that physical links with the same transmission media and transmission rate are “bound” together, making them look like one link logically. This concept is also known

as Trunk. It allows parallel physical links between the switches or between the switch and the server to increase the bandwidth in multiples and simultaneously. As a result, it becomes an import technology in broadening link bandwidth and creating link transmission flexibility and redundancy.

Aggregated link is also called trunk. If a port of the trunk is blocked or faulty, the data packets will be distributed to other ports of this trunk for transmission. If this port recovers, the data packets will be re-distributed to all the normal ports of this trunk for transmission.

ZXR10 2920/2928/2952/2936-FI supports up to 15 aggregation groups. In each aggregation group, the number of links participating in the aggregation does not exceed eight. Links participating in the aggregation must have the same transmission media type and the same transmission rate.

Basic Configuration of LACP

LACP configuration on the switch includes the following contents:

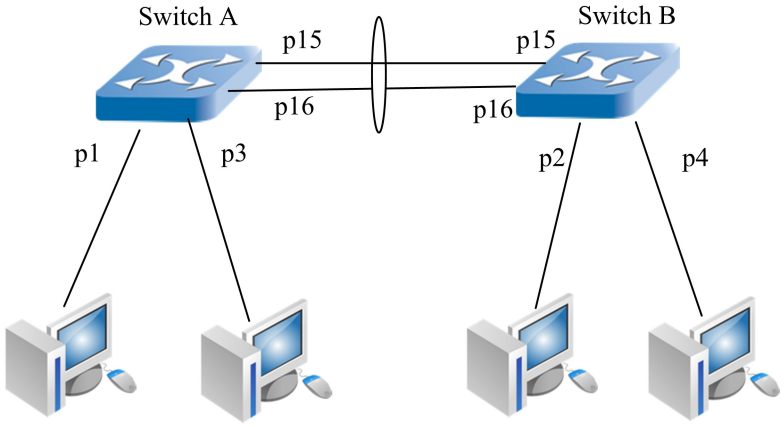
Command	Function
`zte(cfg)#`**set lacp** {**enable**|**disable**}	This enables or disables LACP function. By default, the LACP function is disabled.
`zte(cfg)#`**set lacp aggregator** <*trunkid*>**add port** <*portlist*>	This adds a specified port to LACP aggregation group.
`zte(cfg)#`**set lacp aggregator** <*trunkid*>**delete port** <*portlist*>	This deletes a specified port from LACP aggregation group.
`zte(cfg)#`**set lacp aggregator** <*trunkid*> **mode** {**dynamic**|**static**|**mixed**}	This sets aggregation mode of aggregation group.
`zte(cfg)#`**set lacp port** <*portlist*> **timeout** {**long**|**short**}	This configures the timeout information of the port participating in the aggregation.
`zte(cfg)#`**set lacp port** <*portlist*> **mode** {**active**|**passive**}	This sets the mode used by the port to participate in the aggregation.
`zte(cfg)#`**set lacp priority** <*1-65535*>	This sets the priority of LACP.
`zte(cfg)#`**show lacp**	This displays the LACP configuration information.

Command	Function
zte(cfg)#**show lacp aggregator** [<*trunkid*>]	This displays the aggregation information about the LACP aggregation group.
zte(cfg)#**show lacp port** [<*portlist*>]	This displays the information of the port where the LACP is involved in the aggregation.

LACP Configuration Example

As shown in Figure 48, switch A and switch B are connected through the aggregation port (binding the port 15 and port 16). Port 1 of switch A and port 2 of switch B belong to VLAN2. Port 3 of switch A and port 4 of switch B belong to VLAN3. Members of the same VLAN can communicate with each other.

FIGURE 48 EXAMPLE OF LACP CONFIGURATION



The detailed configuration of switch A is as follows:

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 15-16
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 1 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 3 untag
zte(cfg)#set port 1 pvid 2
zte(cfg)#set port 3 pvid 3
zte(cfg)#set vlan 2-3 enable
```

The detailed configuration of switch B is as follows:

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 3 add port 15-16
zte(cfg)#set lacp aggregator 3 mode dynamic
zte(cfg)#set vlan 2 add trunk 3 tag
zte(cfg)#set vlan 2 add port 2 untag
zte(cfg)#set vlan 3 add trunk 3 tag
zte(cfg)#set vlan 3 add port 4 untag
zte(cfg)#set port 2 pvid 2
```

```
zte(cfg)#set port 4 pvid 3
zte(cfg)#set vlan 2-3 enable
```

The result of showing LACP is as follows:

The results of implementing the following command on the two switches are similar. The result of switch B is omitted. The result of switch A is showed as follows:

```
zte(cfg)#show lacp
Lacp is enabled.
Lacp priority is 32768
PortNum     GroupNum    GroupMode   LacpTime    LacpActive
----------- ----------- ----------- ----------- -----------
15            3           Dynamic       Long         True
16            3           Dynamic       Long         True
zte(cfg)#show lacp aggregator 3
Group 3
            Actor                          Partner
            ------------------------------ --------------------------
Priority   :  32768                          32768
Mac      :  00.d0.d0.fa.29.20                00.d0.d0.fc.88.63
Key      :  258                            258
Ports     :  16, 15                           16, 15
```

The above displaying result proves that link aggregation is successful. If it is not successful, the result is showed as follows when the command of show lacp aggregator 3 is implemented.

```
zte(cfg)#show lacp aggregator 3
  %  Group 3 is not active!
```

Generally, the problem of physical link causes the result. Please check physical link status.

STP Configuration

STP Overview

Spanning Tree Protocol (STP) is applicable to a loop network. It blocks some redundant paths with certain algorithms so that the loop network is pruned into a tree network without any loop, thus avoiding the hyperplasia and infinite loop of packets in the loop network.

Rapid Spanning Tree Protocol (RSTP) is on the basis of common STP, added with the mechanism that the port state can be rapidly changed from Blocking to Forwarding, which increases the topology convergence speed.

Multiple Spanning Tree Protocol (MSTP) is on the basis of RSTP and STP, added with the forwarding processing of frames with VLAN ID. The whole network topology structure can be planned into a Common and Internal Spanning Tree (CIST), which is divided into Common Spanning Tree (CST) and Internal Spanning Tree (IST), as shown in Figure 49.

Many devices enabling MSTP construct MST area in switching network. When the devices satisfy the following conditions, they can be considered to exist in a MST area. A switching network can

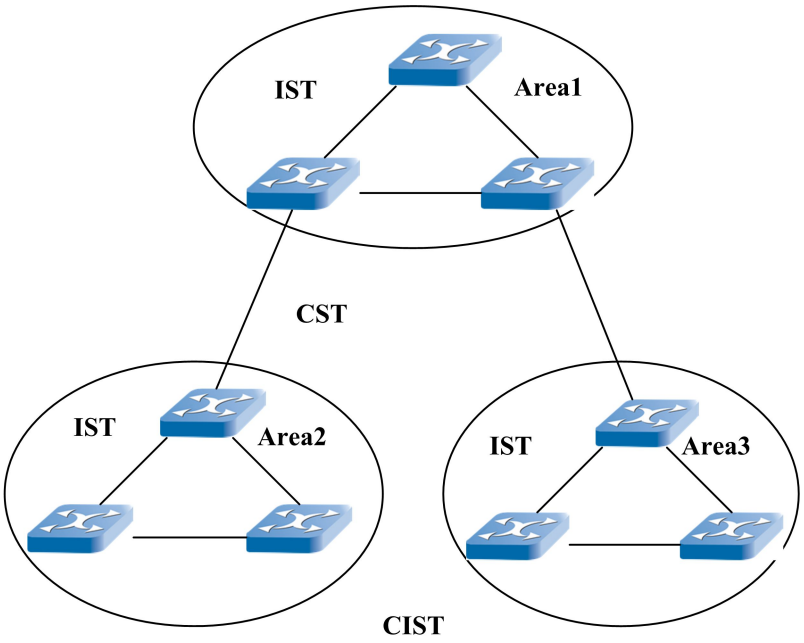
cover many MST areas. User can divide the switches into a MST area by using MSTP commands.

- Same area name.
- Same reversion level.
- Same mapping relationship between VLAN and instance.
- Switches should be connected directly.

There are many spanning trees can be configured in each MSTP area, and they are independent each other. Each spanning tree is Internal Spanning Tree (IST), and it can be called as Multiple Spanning Tree Instance (MSTI). Common Spanning Tree connect all MST areas in switching network. A MST area can be considered as a switch, CST is a spanning tree which is generated by STP and RSTP protocol calculation. All ISTs and CSTs are called as Common and Internal Spanning Tree (CIST). CIST is a single spanning tree to connect all switches.

In this MSTP topology structure, an IST can serve as a single bridge (switch). In this way, CTS can serve as an RSTP for the interaction of configuration information (BPDU). Multiple instances can be created in an IST area and these instances are valid only in this area. An instance is equivalent to an RSTP, except that the instance needs to perform BPDU interaction with bridges outside this area.

FIGURE 49 MSTP TOPOLOGICAL STRUCTURE



Spanning Tree Protocol (STP) can calculate according to the protocol. Ports are divided into different parts:

- Master: The port type is introduced in MSTP protocol. When the multiple different areas exist, the main port is the minimal path cost port point to the root.
- Root: The port that has the minimal cost to root bridge and takes charge in forwarding data to root node. When multiple

ports have the same cost to the root bridge, then the port with the lowest port priority becomes to the root port.

- Designated: The port transmits data to switch downward, and sends STP protocol message to maintain the state of STP.
- Backup: The port receives the STP message, which proves that there exits a loop route to the port itself.
- Alternate: The port receives excess STP protocol message from other equipment. However, when the original link abnormally lost, the port under this state can transfer to transmitting state and maintain the network instead of the port lapsed.
- Edged: The port is used to connect the terminal equipment, such as PC. The port does not participate in calculation before STP is stable, and the state can be switched fast.

According to port role, the state after the calculation being steady is shown in Table 13.

TABLE 13 PORT ROLE AND PORT STATE

Port role	Port state
Master	Forward
Root	Forward
Designated	Forward
Backup	Discard
Alternate	Discard
Edged	Forward

BPDU protect function is for the protection of margin port. The margin port will not receive the protocol message. If there exists vicious protocol attack or Linux virtual bridge, receiving unlawful protocol message will bring to net shocking or topology changing abnormally. The port will be closed after using the protection. After a while, to check the net is normal or not. If it is normal, it will recover to original state.

Root protection is function is for the protection of root switch. In the network that needs to appoint switch as root switch, if there exists vicious protocol attack or Linux virtual bridge, it will bring the change to the root and net abnormal. After using the root protection of the port, if the port receives the protocol information prior to root switch, it will transfer the port to blocking state. This port no longer transmits message, and discards the received protocol message to protect the status of the root switch.

Loop protection function is for the protection of loop net topology. In the network where ring exists, redundant topology will be in the state of backup, and in the state of blocking after the port is steady. If there is no need to transfer to transmission state, it is possible to set port to loop protect. Once the port wants to transform, it will inspire loop protection and set the port to blocking state.

When configuring one port, only one of the three protections can be configured: BPDU protection, root protection and loop protection.

Basic Configuration of STP

In the default configuration, the MSTP only has the instance with ins_id as 0. This instance always exists and user cannot manually delete it. This instance is mapped with VLANs 1 to 4094.

Command	Function
zte(cfg)#**clear stp instance** <*1-15*>	This clears the STP instance.
zte(cfg)#**clear stp instance** <*0-15*> **port** <*portid*> **cost**	This clears the cost value of STP instance port.
zte(cfg)#**clear stp instance** <*0-15*> **trunk** <*trunkid*> **cost**	This clears the trunkcost value of instance.
zte(cfg)#**clear stp name**	This clears the STP area name.
zte(cfg)#**set stp** {**enable**|**disable**}	This enables or disables STP. The default setting is disabled.
zte(cfg)#**set stp name** <*name*>	This sets the area name of MST. The size of the name is no more than 32 characters.
zte(cfg)#**set stp forceversion** {**mstp**|**rstp**|**stp**}	This sets the forced STP type to mstp/rstp/stp. The default forced type is mstp.
zte(cfg)#**set stp instance** <*0-15*>[**add**|**delete**] **vlan** <*vlanlist*>	This sets the mapping relationship between VLAN and instance.
zte(cfg)#**set stp instance** <*0-15*> **priority** <*0-61440*>	This sets the instance bridge priority.
zte(cfg)#**set stp instance** <*0-15*> **port** <*portname*> **priority** <*0-240*>	This sets the instance port priority.
zte(cfg)#**set stp instance** <*0-15*> **trunk** < *trunkid* > **priority** <*0-240*>	This sets the instance trunk priority.
zte(cfg)#**set stp instance** <*0-15*> **port** <*portname*> **cost** <*1-200000000*>	This sets the instance port cost.
zte(cfg)#**set stp instance** <*0-15*> **port** <*portname*> **root-guard** {**enable**|**disable**}	This enables/disables instance port root protection.

Command	Function
zte(cfg)#**set stp instance** <*0-15*> **port** <*portname*>**loop-guard**{**enable**|**disable**}	This enables/disables instance port loop protection.
zte(cfg)#**set stp instance** <*0-15*> **trunk** <*trunkname*> **cost** <*1-200000000*>	This sets instance trunk cost.
zte(cfg)#**set stp instance** <*0-15*> **trunk** <*trunkname*> **root-guard** {**enable**|**disable**}	This enables/disables instance trunk root protection.
zte(cfg)#**set stp instance** <*0-15*> **trunk** <*trunkname*>**loop-guard**{**enable**|**disable**}	This enables/disables instance trunk loop protection.
zte(cfg)#**set stp port** <*portlist*>{**enable**|**disable**}	This enables/disables port stp function.
zte(cfg)#**set stp trunk** <*trunklist*>{**enable**|**disable**}	This enables/disables trunk stp function.
zte(cfg)#**set stp port** <*portlist*> **bpdu-guard**{**enable**|**disable**}	This enables/disables port bpdu protection.
zte(cfg)#**set stp port** <*portlist*> **pcheck**	This sets port stp type check.
zte(cfg)#**set stp bpdu-interval** <*10-65535*>	This sets BPDU protection port linkdown interval, the default is 100, the unit is s.
zte(cfg)#**set stp port** <*portlist*> **linktype** {**point-point**|**shared**}	This sets instance port Linktype.
zte(cfg)#**set stp trunk** <*trunklist*> **linktype** {**point-point**|**shared**}	This sets instance trunk Linktype.
zte(cfg)#**set stp port** <*portlist*> **packettype** {**IEEE**|**CISCO**|**HUAWEI**|**HAMMER**|**extend**}	This sets instance port packet type.
zte(cfg)#**set stp trunk** <*trunkid*> **packettype** {**IEEE**|**CISCO**|**HUAWEI**|**HAMMER**|**extend** }	This sets instance trunk packet type.
zte(cfg)#**set stp hellotime** <*1-10*>	This sets STP notification interval, the default is 2, unit is s.
zte(cfg)#**set stp forwarddelay** <*4-30*>	This sets STP forwarding delay time, the default is 15, unit is s.
zte(cfg)#**set stp agemax** <*6-40*>	This sets STP aging time, the default is 20, unit is s.

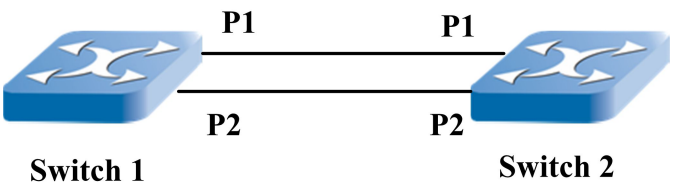
Command	Function
zte(cfg)#**set stp hopmax** <*1-40*>	This sets the maximum number of hop between any two terminals of MST. The default is 20.
zte(cfg)#**set stp revision** <*0-65535*>	This sets version number of MST.
zte(cfg)#**set stp edge-port** {**add**|**delete**} **port** <*portlist*>	This adds/deletes edge port of STP.
zte(cfg)#**set stp hmd5-digest** {**CISCO**|**HUAWEI**}<*0,0x00..0-0xff..f*>	This sets stp hmd5 digest.
zte(cfg)#**set stp hmd5-key** {**CISCO**|**HUAWEI**}<*0,0x00..0-0xff..f*>	This sets stp hmd5 key.
zte(cfg)#**show stp**	This views STP information.
zte(cfg)#**show stp instance** [<*0-15*>]	This views information of STP instance.
zte(cfg)#**show stp port** [<*portlist*>]	This views information of STP port.
zte(cfg)#**show stp trunk** <*trunklist*>	This views information of STP trunk.

Configuration Example

STP Configuration Example

As shown in Figure 50, configure the STP function of switch 1 and switch 2 , take switch 1 as the root bridge and block a redundant port in the loop. It realizes loop protection and link backup between switches.

FIGURE 50 STP CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#set stp enable
/*enable the stp protocol of switch1 and switch2*/
zte(cfg)#set stp forceversion stp
/*set STP forceversion as stp*/
zte(cfg)#show stp instance
/*show the STP state of switch1 in the system view*/
```

```
  Spanning tree enabled protocol stp
  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s): 15
  Reg  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  RemainHops     : 20
  BridgeID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s): 15          MaxHops  : 20
  Interface PortId Cost  Status Role  Bound GuardStatus
  -------    ------  --------  -------  --------  -----  ----
   1   128.1  200000  Forward Designated  SSTP   None
   2   128.2  200000  Forward Designated  SSTP  None
zte(cfg)#show stp instance
/*show the STP state of switch2 in the system view*/
  Spanning tree enabled protocol stp
  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s):15
 Reg  RootID:
  Priority       : 32768       Address  : 00.d0.d0.29.52.06
  RemainHops     : 20
  BridgeID:
  Priority       : 32768       Address  : 00.d0.d0.29.52.06
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s): 15          MaxHops  : 20
  Interface  PortId  Cost    Status     Role     Bound   GuardStatus
  ---------    ------   ---------  -------     ----------    -----
   1      128.1  200000   Forward   Root     SSTP     None
   2      128.2  200000   Discard   Alternate  SSTP     None
```

RSTP Configuration Example

As shown in “STP Configuration Example”, configure the RSTP function of switch 1 and switch 2 , take switch 1 as the root bridge and block a redundant port in the loop. It realizes loop protection and link backup between switches.

Configuration of switch:

```
zte(cfg)#set stp enable
/*enable STP protocol of switch1 and switch2*/
zte(cfg)#set stp forceversion rstp
/*set forceversion of stp as rstp*/
zte(cfg)#show stp instance
/*show the STP state of switch1 in system view*/
 Spanning tree enabled protocol rstp
  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s): 15
  Reg  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  RemainHops     : 20
  BridgeID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s): 15          MaxHops  : 20
  Interface  PortId   Cost      Status  Role      Bound   GuardStatus
  ---------   ------     ---------    -------   ----------     -----
  1       128.1   200000   Forward  Designated  RSTP     None
  2       128.2   200000   Forward  Designated  RSTP     None
zte(cfg)#show stp instance
 /*show the STP state of switch2 in system view*/
  Spanning tree enabled protocol rstp
  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
```

```
  HelloTime(s)    : 2           MaxAge(s): 20
  ForwardDelay(s):15
  Reg  RootID:
  Priority        : 32768       Address  : 00.d0.d0.29.52.06
  RemainHops      : 20
  BridgeID:
  Priority        : 32768       Address  : 00.d0.d0.29.52.06
  HelloTime(s)    : 2           MaxAge(s): 20
  ForwardDelay(s): 15           MaxHops  : 20
  Interface  PortId    Cost     Status      Role   Bound  GuardStatus
  ---------    ------    ---------    -------  ----------    -----
    1       128.1  200000   Forward   Root    RSTP   None
    2       128.2  200000   Discard   Alternate  RSTP  None
```

MSTP Configuration Example

As shown in "STP Configuration Example", configure the MSTP of switch1 and switch2 (They are in the same MST area) to realize link backup and block the loop in the net. The configuration is as follows: establish mapping between instance 1 and service VLAN10-20; set Name as zte, Revision as 10. Take switch1 as the root bridge in instance 1.

Configuration of switch:

```
zte(cfg)#set stp enable
/*enable the stp protocol of switch1 and switch2*/
zte(cfg)#set stp forceversion mstp
/*set the STP forceversion as mstp */
zte (cfg)#set stp name zte
/*set switch1 and switch2 in the same area*/
zte(cfg)#set stp revision 10
zte(cfg)#set stp instance 1 add vlan 10-20
zte(cfg)#show stp
 /*show the STP configure of switch1 and switch2 in system view*/
  The spanning_tree protocol is enabled!
  The STP ForceVersion is MSTP !
  Revision: 10     Name: zte
  Cisco key:     0x13ac06a62e47fd51f95d2ba243cd0346
  Cisco digest:  0x00000000000000000000000000000000
  Huawei key:    0x13ac06a62e47fd51f95d2ba243cd0346
  Huawei digest: 0x00000000000000000000000000000000
  Instance VlanMap
  -------- -------------------
  0        1-9, 21-4094
  1        10-20
zte(cfg)#show stp instance
 /*show the STP state of switch1 in system view*/
MST00
  Spanning tree enabled protocol mstp
  RootID:
  Priority        : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)    : 2           MaxAge(s): 20
  ForwardDelay(s): 15
  Reg  RootID:
  Priority        : 32768       Address  : 00.d0.d0.02.00.54
  RemainHops      : 20
  BridgeID:
  Priority        : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)    : 2           MaxAge(s): 20
  ForwardDelay(s): 15           MaxHops  : 20
  Interface PortId Cost Status Role   Bound GuardStatus
  --------- ------ ------ ---- -----  -----  ----------
  1      128.1  200000    Forward Designated   MSTP  None
  2      128.2  200000    Forward Designated   MSTP  None
 MST01
  Spanning tree enabled protocol mstp
  RootID:
  Priority        : 32769       Address     : 00.d0.d0.02.00.54
  HelloTime(s)    : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15           RemainHops  : 20
```

```
  BridgeID:
  Priority       : 32769       Address     : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          MaxHops     : 20
  Interface PortId Cost  Status Role      GuardStatus
  --------- -----  ----  ----- -----     -----------
 1       128.1   200000    Forward  Designated  None
  2       128.2   200000    Forward  Designated  None
zte(cfg)#show stp instance
/*show the STP state of switch2 in system view*/
MST00
  Spanning tree enabled protocol mstp
  RootID:
  Priority       : 32768       Address  : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s): 20
                          ForwardDelay(s):15
    Reg  RootID:
  Priority       : 32768       Address  : 00.d0.d0.29.52.06
  RemainHops   : 20
  BridgeID:
  Priority       : 32768       Address  : 00.d0.d0.29.52.06
  HelloTime(s)   : 2           MaxAge(s): 20
  ForwardDelay(s): 15          MaxHops  : 20
  Interface  PortId  Cost  Status Role   Bound GuardStatus
  ---------  ------  -----  ----- -----   -----  ---------
  1       128.1     200000   Forward  Root      MSTP  None
  2       128.2     200000   Discard  Alternate   MSTP  None
MST01
  Spanning tree enabled protocol mstp
  RootID:
  Priority       : 32769       Address     : 00.d0.d0.02.00.54
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s):15          RemainHops  : 19
  BridgeID:
  Priority       : 32769       Address     : 00.d0.d0.29.52.06
  HelloTime(s)   : 2           MaxAge(s)   : 20
  ForwardDelay(s): 15          MaxHops     : 20
 Interface PortId   Cost  Status   Role    GuardStatus
  --------- ------ ------ ------- ------    ----------
   1     128.1     200000  Forward     Root       None
   2     128.2     200000  Discard     Alternate    None
```

ZESR Configuration

ZESR Overview

ZESR Introduction

With the integration of data, voice , video and IP, the demand for network reliability and network fault convergence time are raised in the recent years. To shorten the time of network fault convergence, ZTE provides ZESR (ZTE Ethernet Smart Ring).

ZESR is based on EAPS (RFC 3619) and improved on it. ZESR checks if the ring is proper and ensures that there is only one logical link between any two nodes, which effectively prevents the broadcast storm caused by data loop. When there is a fault on link or device of Ethernet ring, logic route will be switched quickly to ensure the service recover soon. ZESR protocol is more simple

than STP protocol and the topology convergence speed is more fast.

ZESR Related Concepts

1. ZESR Ring

   A ZESR ring physically corresponds to an Ethernet ring topology. A ZESR area consists of multiple ZESR rings. One ring is the major-level, others are the segment linking with the major-level. If there is only one ring in ZESR area, then it is the main-level.

2. ZESR Control VLAN

   Each ZESR area has a control VLAN. The ZESR protocol message is transmitted in the control VLAN.

3. ZESR Protected VLAN

   Each ZESR area has multiple protect VLANs. The users' service is transmitted in the protect VLAN. Realize the service traffic protection in layer-2 by the link switch of ZESR Protected Vlan.

4. Master Node

   Master node is the primary control node. The primary ring and the segment of each level have a node respectively (It can be combined to one, master edge-port). It takes charge in the control of the primary ring and the segment of each level.

5. Transmission Node

   The nodes except the master node in ZESR ring are transmission node. It mainly assists the master to do loop inspection and service switching.

6. Edge Node

   The node connects with more than 2 levels in ZESR ring is called edge node. The edge node can be transmission node (contains 2 ports), master node (contains 2 ports) or assistant port (contains 1 port).

7. Assistant Node

   The assistant port is also edge port. It is the transmission node that has only one port in the relative segment. It mainly assists the master node to achieve service switching for the segment. As shown in "ZESR Multi-ring Multi-domain Design Figure", major ring is composed of S1, S2, S3 and S4. Of which S1 is master node, others are transmission node. Level 1 segment 1 is composed of S3, S4, S5 and S6. Of which S3 and S4 are assistant nodes, S5 is master node, S6 is transmission node. Level 1 segment 2 is composed of S3, S4 and S7. Of which S3 and S4 are assistant nodes, S7 is master node.

8. Smart-link node

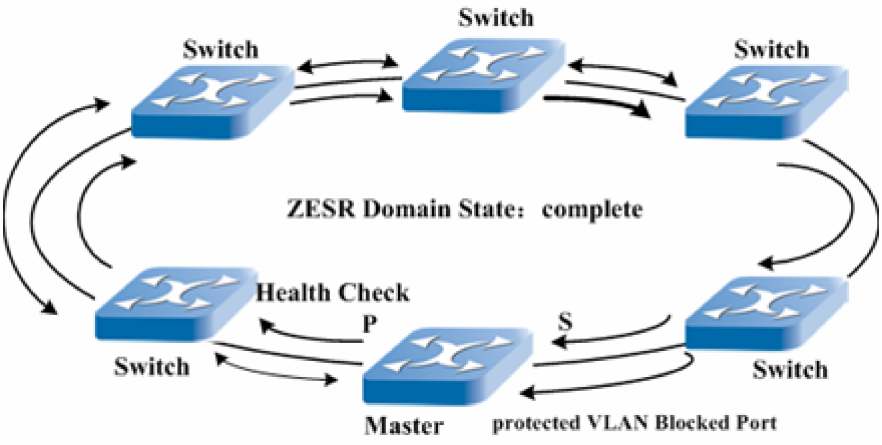
   The smart-link is a simple expansion for the former ZESR function and realizes the protection for key service link. As shown in "SMART-LINK", when the link goes wrong, it can switch automatically and carry out malfunction response in time.

Single-Ring Single-Domain ZESR

ZESR Domain

ZESR domain is an example of ZESR protocol. It is in an Ethernet ring and consists of master node, transit node and control VLAN. As shown in Figure 51, each node is 2900 switch. All the nodes form a ring. The MASTER switch is the master node.

FIGURE 51 ZESR RUNNING STATE WHEN THE RING IS "COMPLETE STATE"



ZESR Domain sets a control VLAN composed of all the ports in the ring. The protected VLAN must contain all the above ports.

ZESR Domain sets a master and multi transit nodes. Each node connects with the ring with two ports: primary port and secondary port.

ZESR Loop Detection Mode

1. Master of ZESR Domain sends HEALTH packet from the primary port in cycle. If the loop link is complete state (the loop is connected), then HEALTH packet is received by the secondary port, if the secondary port does not receive the HEALTH packet, then the link state is link failure.
2. When there is malfunction somewhere, the adjacent node detects the malfunction and informs the master. The loop is link failure.

   As shown in Figure 51, the two interfaces of master are: primary and secondary. The loop port is blocked when master initializes. The secondary port is blocked when the master detects the normal link. If master detects the disconnection of the link, then it forwards the secondary port. The loop port is blocked when the transit initializes.

ZESR Malfunction Recovery

Even if the loop is link failure, the primary port of master also sends HEALTH packet in cycle. If the secondary port receives HEALTH packet, then the loop state is link restore.

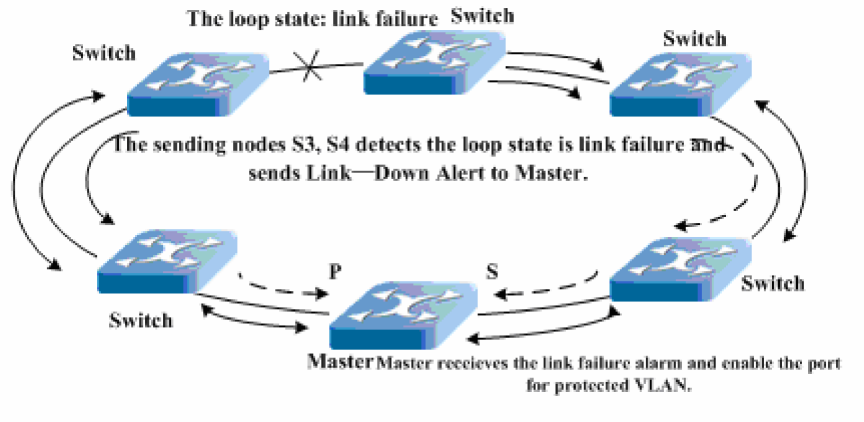
- When the loop is complete state

  As shown in Figure 51, master blocks secondary port, so as to prevent the uncontrolled Ethernet frame in protected VLAN. This cuts the loop logically and avoids the broadcast in protected VLAN.

- When the loop is link failure

As shown in Figure 52, master opens the secondary port to make the data transit through secondary port.

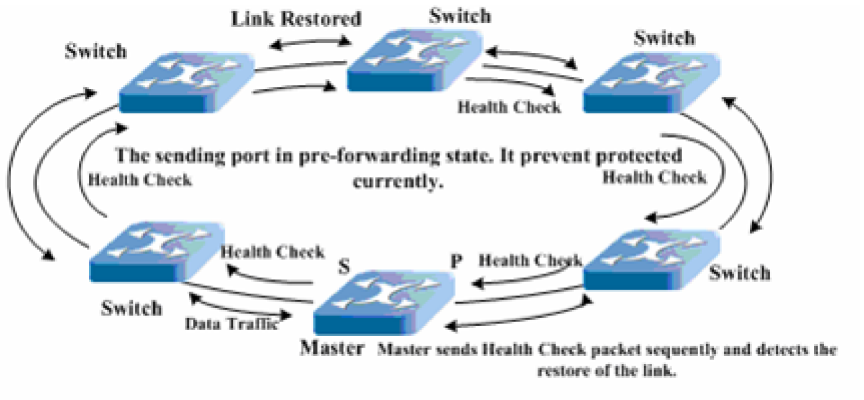
FIGURE 52 ZESR RUNNING STATE WHEN THE RING IS "LINK FAILURE"


The loop state: link failure
Switch
Switch
Switch
The sending nodes S3, S4 detects the loop state is link failure and sends Link—Down Alert to Master.
P
S
Switch
Switch
Master
Master reccieves the link failure alarm and enable the port for protected VLAN.

- When the loop is link restore

  As shown in Figure 53, master detects the link recovery, blocks the secondary port and sets lop as complete state.

FIGURE 53 ZESR RUNNING STATE WHEN THE RING IS "LINK RESTORE"



Multi-Ring Multi-Domain ZESR

Principle of Multi-Ring Multi-Domain ZESR

ZESR domain consists of many switches, which are configured with the same domain ID, control VLAN and protection VLAN. These switches are interconnected. One or more EAPS domains exist on a physical loop. Each EAPS domain defines its master node, transmission node and assistant node (the description of related concepts refers to "ZESR Introduction").

FIGURE 54 MULTI-RING MULTI-DOMAIN

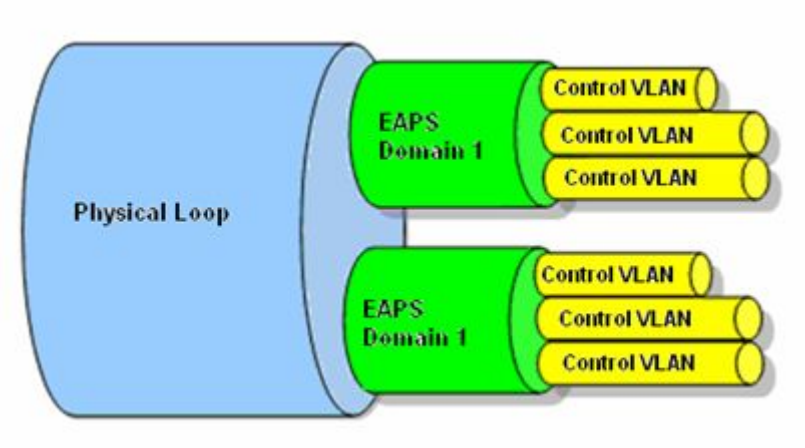
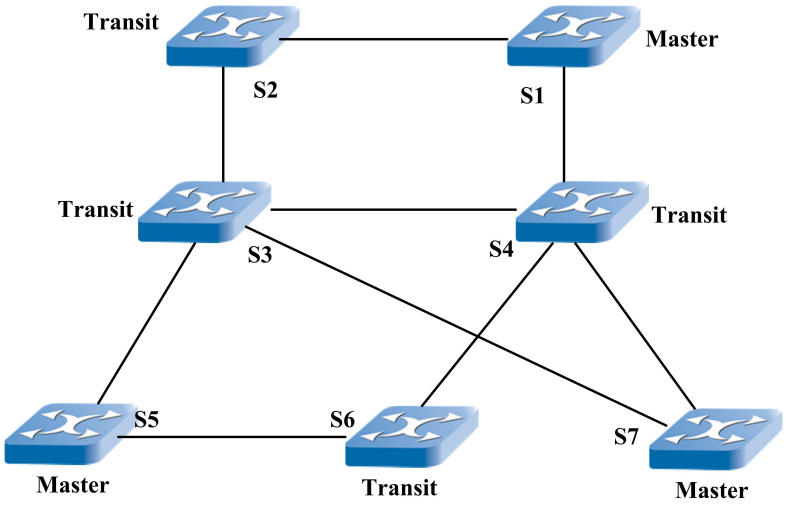


FIGURE 55 ZESR MULTI-RING MULTI-DOMAIN DESIGN FIGURE



Basic Operation Principle of Non Level 0 Segment Link

Hierarchical ZESR technology is brought into the complex network. The running of ZESR protocol on segment link of one level is based on that the upper level primary ring or segment link is not down.

As shown in Figure 56, S3~S6 compose the segment links of level 1 segment 1, where S3 and S4 are assistant nodes and S5 is the master node. S3 and S4 can always intercommunicate with each other via primary ring. If all links where S3, S4, S5 and S6 locate on segment 1 of level 1 are up, master node S5 will block its secondary port, and if the states of some links are Down, the secondary port of the master node will be enabled.

FIGURE 56 NON LEVEL 0 SEGMENT LINK

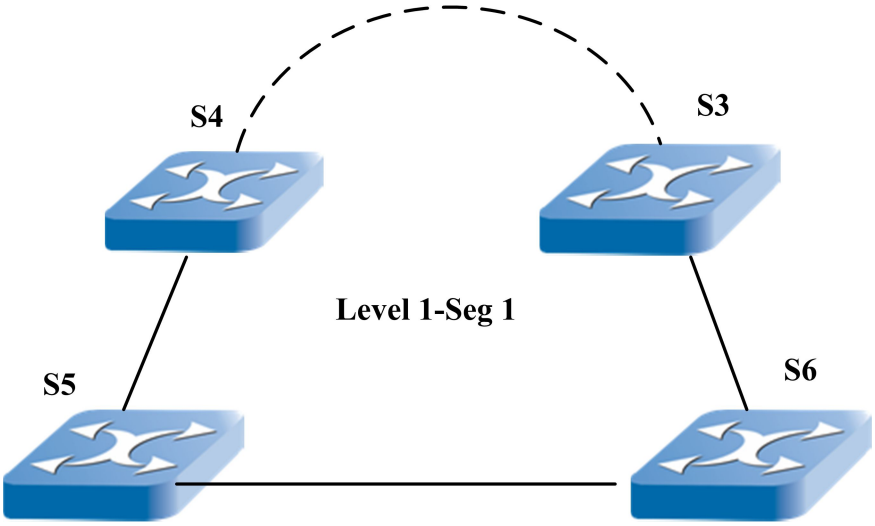
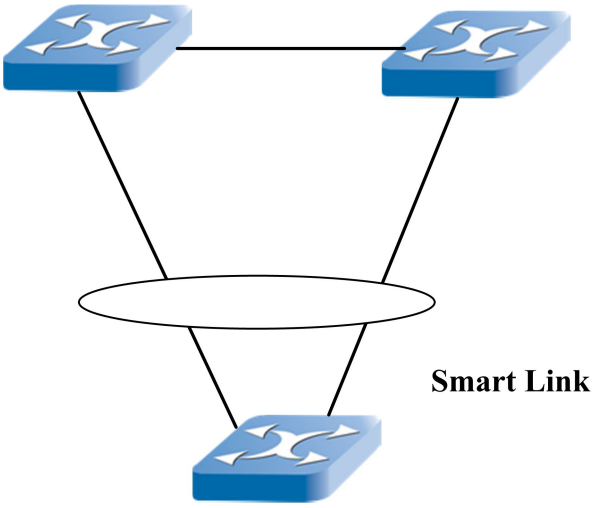


FIGURE 57 SMART-LINK



The Function of Master Node on Primary Ring

One master node exists on primary ring of one ZESR domain. As shown in Figure 55, such as master node S1 is both the initiator of detection of ring network state and the decision-maker for operation after topology changing of primary ring.

The Function of Transit Node

Transit node is used to monitor the state of direct-connect ZESR link and notify the link change to master node, who will make decision for processing.

The Function of Assistant Node

Assistant node is also the border node, and transit node with only one port on corresponding segment link. It is mainly used to monitor the state of direct-connect ZESR, notify the link change to master node and meanwhile monitor the state of master node on segment link.

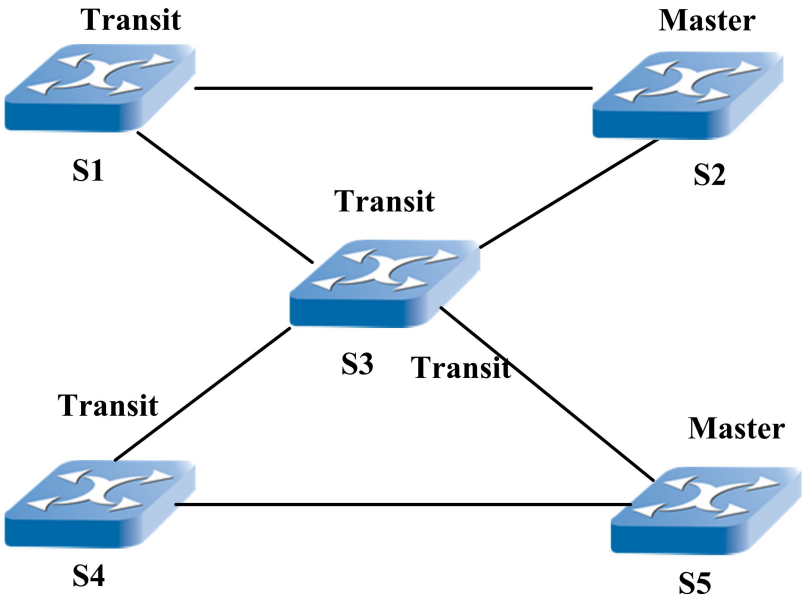
The Function of Multi-Domain

Multiple domains are supported on one segment of link, realizing traffic sharing.

ZESR Tangent Ring

For the reason that ZESR edge-node has heavy burden, ZESR tangent ring adopts the design of using multi ctrl vlans to protect the same group of protected vlans.

FIGURE 58 TANGENT RING DESIGN FIGURE



As shown in Figure 58, the ring composed by S1, S2, S3 and the ring composed by S3, S4, S5 are tangent at S3. The two rings belong to different areas, but they protect the same protected vlans.

Configuration Notice

- No more than 4 areas in one node
- No more than 3 layers in one node
- No more than 3 layers in one area
- No more than 4 lower layer access ports in one node
- No more than 8 ZESR ports in one node

Caution:

When the protocol port of ZESR node is enabled and configured (including master and slave port, edge port, access port), other services, such as adding aggregation port group, enabling port security, port rate limit and enabling loop detection cannot be configured on this protocol port.

Basic Configuration of ZESR

1. To set the node attribute in ZESR domain major level, use the following command.

Function	Command
zte(cfg)#**set zesr domain**<*domainId*> **major-level mode** {**master** | **transit** | **edge-master** | **edge-transit**}	This sets the node attribute in ZESR domain main level.

The parameter **domain**<*domainId*>: ZESR Domain ID, the range is 1-4.

The parameter **mode**: node mode.

The parameter **{master | transit | edge-master | edge-transit}**: They are the master node, transition node, segment link (edge) master node and segment link (edge) transition node respectively.

For edge node, level-id and seg-id represent high-level ring.

2. To set the node attribute in ZESR domain sub ring, use the following command.

Command	Function
zte(cfg)#**set zesr domain**<*domainId*> **level**<*levelId*> **segment**<*segId*> **mode** {**master** | **transit** | **edge-master** | **edge-transit**}	This sets the node attribute in ZESR domain sub ring.

The parameter **domain**<*domainId*>: ZESR Domain ID the range is 1-4.

The parameter **level**<*levelId*>: level ID, the range is 1-2.

The parameter **segment**<*segId*>: Segment link ID, the range is 1 to 4.

The parameter **mode**: The node mode.

The parameter **{master | transit | edge-master | edge-transit}**: They are the master node, transition node, segment link (edge) master node and segment link (edge) transition node respectively.

For edge node, level-id and seg-id represent high-level ring.

3. To delete ZESR domain, use the following command.

Command	Function
zte(cfg)#**clear zesr domain** <*domainId*>	This deletes ZESR domain.

4. To add or delete the primary and the secondary ports, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*>{**add**|**delete**}{**primary-port** | **primary-trunk** | **secondary-port** | **secondary-trunk**}<*portId* | **trunkId**>	This adds or deletes the primary and secondary ports .

5. To add/delete and configure the edge port, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*> **level** <*levelId*> **seg** <*segId*>{**add** | **delete**}{**edge-port** | **edge-trunk**}<*portId* | **trunkId**>[**notmaster** | **master**]	This adds/deletes and configures the edge port.

The parameter **[notmaster|master]** is used for the combination of master nodes belonging to the various layers. The port attribute is that the edge port can send health frame as master node in fixed time to check the related packet and switch the link state. This attribute can only be set in the node with attribute EDGE_MASTER.

6. To add/delete control VLAN in ZESR domain, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*>{**add** | **delete**} **control-vlan** <*vlanId*>	This adds/deletes VLAN in ZESR domain.

7. To add/delete the MSTP instance that the service VLAN belongs, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*>{**add** | **delete**} **protect-instance** <*instanceId*>	This adds/deletes the MSTP instance that the service VLAN belongs.

8. To configure the interval for sending hello packet and timeout interval, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*> **hello-timer** <*1-3*> **fail-timer** <*3-9*>	This configures the interval for sending hello packet and timeout interval.

The parameter **hello-timer** : The sending time interval. The unit is second and it is 1s by default.

The parameter **fail-timer** : The timeout. The unit is second and it is 3s by default.

Only the node whose attribute is master or edge-master can be configured.

9. To set preup and preforward time on major level ring, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*> **major-level preforward-timer** <*3-600*> **preup-timer** <*0-500*>	This sets preup and preforward time on major level ring. By default, preforward-timer is 3s, preup-timer is 0s.

The main-level preforward-time and preuptime must satisfy the following condition: preforwardtime - preuptime >= 3 !

10. To set preup and preforward time on non major level ring, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*> **level** <*levelid*> **seg** < *segmentid* > **preforward-timer** <*3-600*> **preup-timer** <*0-500*>	This sets preup and preforward time on non major level ring. By default, preforward-timer is 3s, preup-timer is 0s.

For both the main level and the level of all the nodes in the zesr domain, the preforward and preup time must be the same

11. To enable or disable ZESR function in ZESR domain, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId* >{**enable** | **disable**}	This enables or disables ZESR function in ZESR domain.

12. To set ZESR smart-link node, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*> **mode smart-link**	This sets ZESR smart-link node.

13. To set ZESR SMART-LINK access port, use the following command.

Command	Function
zte(cfg)#**set zesr domain** <*domainId*>{**add** | **delete**}{**access-port** | **access-trunk**}<*portId* | **trunkId**>	This sets ZESR SMART-LINK access port.

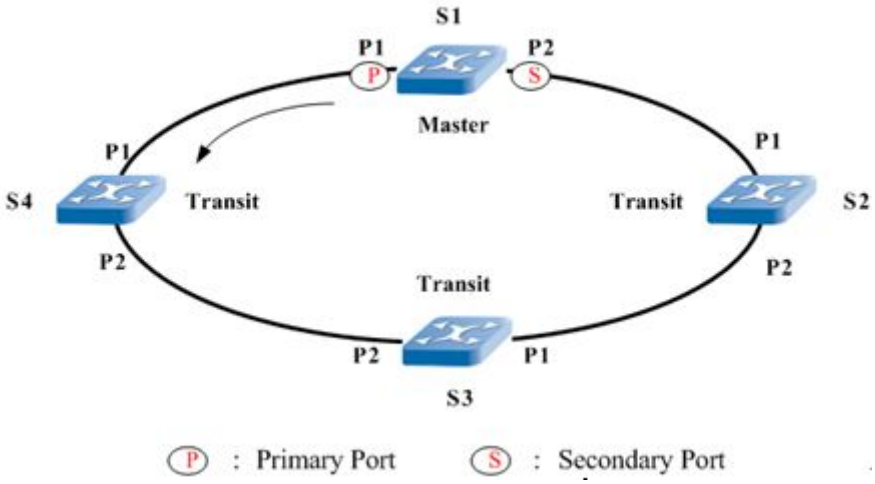
14. To display ZESR configuration, use the following command.

Command	Function
zte(cfg)#**show zesr domain** [<*domainId*>]	This displays ZESR configuration.

ZESR Configuration Example

ZESR Single Ring Networking Example

FIGURE 59 ZESR SINGLE RING NETWORKING



The single ring networking composed by four switches is shown above. S1 is Master node, P1 is Primary Port, P2 is Secondary Port. S2~S4 are Transit nodes.

The protect instance in the ring is 1, the protected data VLAN is 100 and the protocol control VLAN is 4000.

Node configuration of switch:

1. S1 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1,2 untag
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

   ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode master
```

```
zxr10(cfg)#set zesr domain 1 enable
```

2. S2~S4 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

   ZESR:

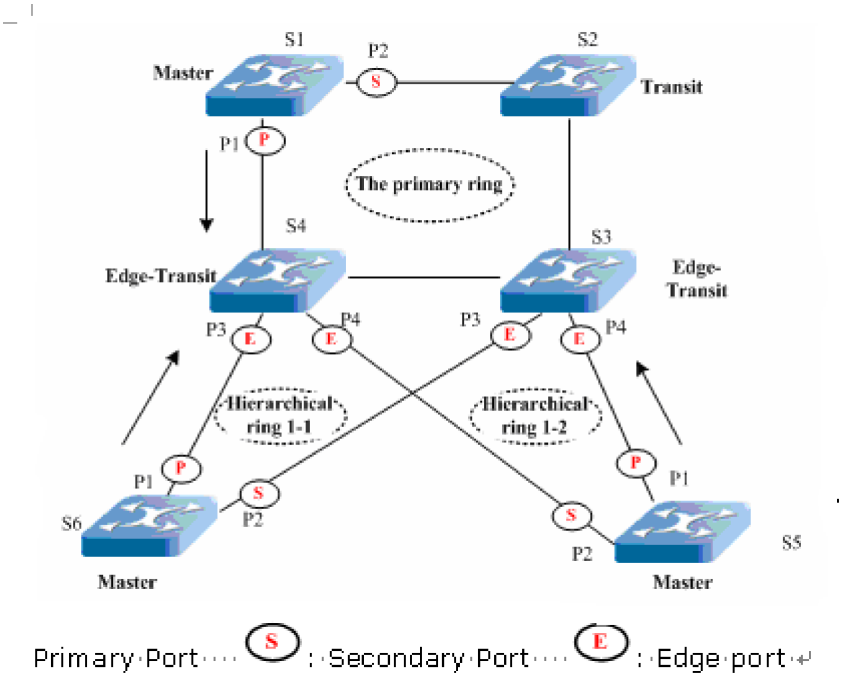
```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode transit
zxr10(cfg)#set zesr domain 1 enable
```

Configuration descriptions are shown below.

1. ZESR port in control VLAN must be configured as tag port.
2. Before enabling ZESR function, STP function must be enabled.
3. The primary port and the secondary port in master node are different on function. Normally, the primary port is set as forwarding status, but the secondary port is set as blocking status.
4. The primary port and the secondary port in transit node are the same on function. Normally, they are both set as forwarding status.

ZESR Multi-Ring Networking Example

FIGURE 60 ZESR MULTI RING NETWORKING



This example describes how to configure ZESR multi ring networking domain. The multi ring networking composed of 6 switches is shown above. There are one ZESR primary ring and two hierarchical rings.

1. The primary ring is composed of nodes S1~S4. S1 is Master, P1 is the Primary Port, P2 is the Secondary Port, S2 is the Transit node, S3~S4 are Edge-Transit node, P3 and P4 are the edge-port of the two hierarchical rings.
2. The link 1 of hierarchical ring is composed of S6, S3 and S4. S6 is the Master, P1 is the Primary Port, P2 is the Secondary Port, S3 and S4 are the assisting nodes.
3. The link 2 of hierarchical ring 1 is composed of S5, S3 and S4. S5 is the Master, P1 is the Primary Port, P2 is the Secondary Port, S3 and S4 are the assisting nodes.

The protect instance in the ring is 1, the protected data is VLAN 100 and the protocol VLAN is VLAN 4000.

node configuration of switch:

1. S1 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

   ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode master
zxr10(cfg)#set zesr domain 1 enable
```

2. S2 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

   ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode transit
zxr10(cfg)#set zesr domain 1 enable
```

3. S3 and S4 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1-4
zxr10(cfg)#set vlan 4000 add port 1-4 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1-4 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

   ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode edge-transit
zxr10(cfg)#set zesr domain 1 level 1 segment 1 add edge-port 3 notmaster
zxr10(cfg)#set zesr domain 1 level 1 segment 2 add edge-port 4 notmaster
zxr10(cfg)#set zesr domain 1 enable
```

4. S5 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

   ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 level 1 segment 2 mode master
zxr10(cfg)#set zesr domain 1 enable
```

5. S6 node

VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

ZESR:

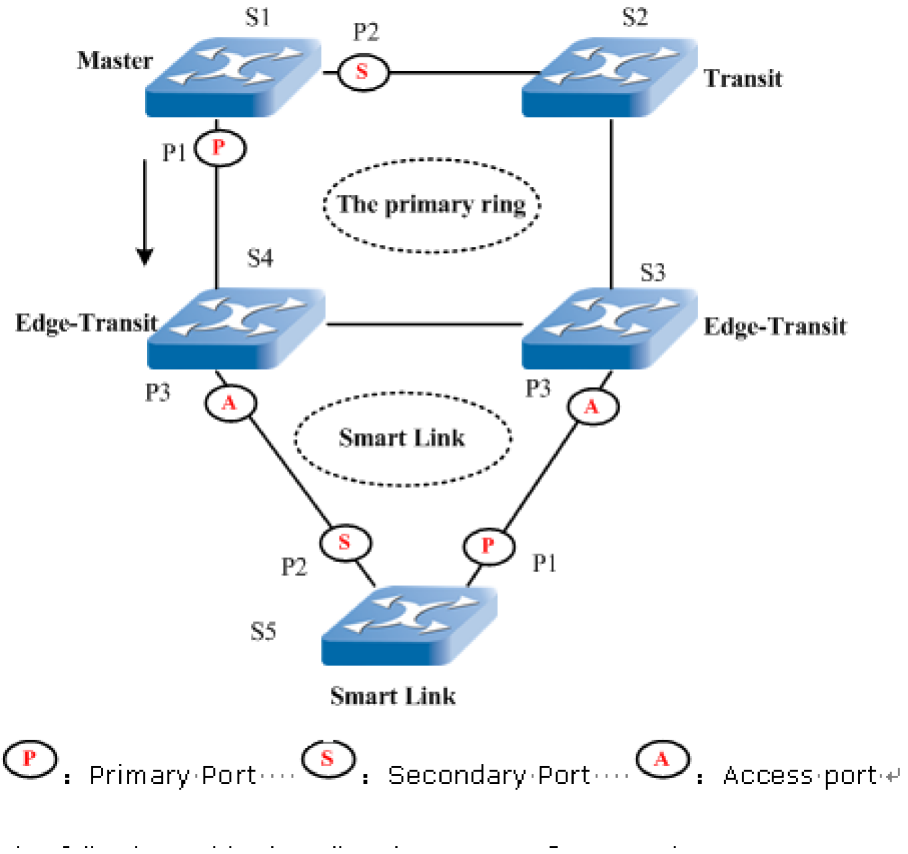
```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 level 1 segment 1 mode master
zxr10(cfg)#set zesr domain 1 enable
```

Configuration descriptions are shown below.

1. The intersecting node of the primary ring and the hierarchical ring must be Edge-Port or Edge-Transit.
2. The port connecting the primary ring and the hierarchical ring must be Edge-Port.
3. The edge-port has two attributes: not Master and Master. The attribute not Master is used in the condition that the master of the hierarchical ring exists. Master is used in the condition that the master does not exist and the edge-port master serves as the master.
4. The edge-port with Master attribute must be set on edge-master.

ZESR Smart Link Networking Example

FIGURE 61 SMART LINK NETWORKING



This example describes how to configure ZESR smart link networking domain. The smart link networking composed of 5 switches is shown above. There are one ZESR primary ring and one smart link node.

1. The primary ring is composed of nodes S1~S4. S1 is Master, P1 is the PrimaryPort, P2 is the SecondaryPort, S2 is the Transit node, S3~S4 are Edge-Transit node, P3 is the Access port using for Smart Link.
2. S5 is the Smart Link node. P1 is the PrimaryPort. P2 is the SecondaryPort.

The protect instance in the ring is 1, the protected data is VLAN 100 and the protocol VLAN is VLAN 4000.

node configuration of switch:

1. S1 node

   VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

   STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
```

```
zxr10(cfg)#set stp enable
```

ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode master
zxr10(cfg)#set zesr domain 1 enable
```

2. S2 node

VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode transit
zxr10(cfg)#set zesr domain 1 enable
```

3. S3 and S4 nodes

VLAN:

```
zxr10(cfg)#set vlan 100 add port 1-3
zxr10(cfg)#set vlan 4000 add port 1-3 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1-3 pvid 100
```

STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 major-level mode edge-transit
zxr10(cfg)#set zesr domain 1 add access-port 3
zxr10(cfg)#set zesr domain 1 enable
```

4. S5 node

VLAN:

```
zxr10(cfg)#set vlan 100 add port 1, 2
zxr10(cfg)#set vlan 4000 add port 1, 2 tag
zxr10(cfg)#set vlan 100, 4000 enable
zxr10(cfg)#set port 1, 2 pvid 100
```

STP:

```
zxr10(cfg)#set stp instance 1 add vlan 100
zxr10(cfg)#set stp enable
```

ZESR:

```
zxr10(cfg)#set zesr domain 1 add control-vlan 4000
zxr10(cfg)#set zesr domain 1 add protect-instance 1
zxr10(cfg)#set zesr domain 1 add primary-port 1
zxr10(cfg)#set zesr domain 1 add secondary-port 2
zxr10(cfg)#set zesr domain 1 mode smart-link
```

```
zxr10(cfg)#set zesr domain 1 enable
```

Configuration descriptions are shown below.

1. The intersecting node of the primary ring and the Smart Link node must set as Edge-Master or Edge-Transit.
2. The port connecting the primary port and Smart Link must set as Access-Port.
3. The Smart Link can be used with the hierarchical ring at the same time.

IGMP Snooping Configuration

IGMP Snooping Overview

Because the multicast address cannot appear in the source address of the packet, the switch cannot learn the multicast address. When the switch receives a multicast message, it broadcasts the message to all the ports in the same VLAN. If measure is not taken, unwanted multicast message may be spread to each node of the network, thus causing a great waste of network bandwidth resource.

With the IGMP Snooping function, the IGMP communication between the host and router is snooped, so that the multicast packets are sent to the ports in the multicast forwarding table, instead of all ports. This restricts the wide spread of multicast messages in the LAN switch, reduces the waste of network bandwidth, and improves the utilization rate of the switch.

Basic Configuration of IGMP Snooping

Configuration of IGMP Snooping on the switch includes the following contents:

Command	Function
`zte(cfg)#`**set igmp snooping** {**enable**|**disable**}	This enables or disables IGMP Snooping function. This function is disabled by default.
`zte(cfg)#`**set igmp snooping add vlan** <*vlanlist*>	This adds the IGMP Snooping function for the specified VLAN.

Command	Function
zte(cfg)#**set igmp snooping delete vlan** <*vlanlist*>	This deletes the IGMP Snooping function for the specified VLAN.
zte(cfg)#**set igmp snooping query vlan** <*vlanlist*>{**enable**|**disable**}	This enables or disables the IGMP snooping query function for the specified VLAN.
zte(cfg)#**set igmp snooping vlan** <*vlanname*>**add group** <*A.B.C.D*>	This adds static multicast group based on VLAN.
zte(cfg)#**set igmp snooping vlan** <*vlanname*> **delete group** <*A.B.C.D*>	This deletes static multicast group based on VLAN.
zte(cfg)#**set igmp snooping vlan** <*1-4094*>**add group** <*A.B.C.D*>[**port** <*portlist*>|**trunk** <*trunklist*>]	This adds static multicast group based on port or aggregation port into VLAN. The number of groups of multicast IP address is no more than 64.
zte(cfg)#**set igmp snooping vlan** <*1-4094*> **delete group** <*A.B.C.D*>[**port** <*portlist*>|**trunk** <*trunklist*>]	This removes static multicast group based on port or aggregation port from the specified multicast snooping VLAN.
zte(cfg)#**set igmp snooping vlan** <*1-4094*> **add smr** [**port** <*portlist*>|**trunk** <*trunklist*>]	This adds static multicast router port or static route aggregation port to a VLAN.
zte(cfg)#**set igmp snooping vlan** <*1-4094*> **delete smr** [**port** <*portlist*>|**trunk** <*trunklist*>]	This deletes static route port or static route aggregation port from the specified multicast monitor VLAN.
zte(cfg)#**set igmp snooping add maxnum** <*1-256*> **vlan** <*vlanlist*>	This configures the maximum multicast group number of the specified multicast monitor VLAN. The default value is 256.
zte(cfg)#**set igmp snooping delete maxnum vlan** <*vlanlist*>	This deletes maximum multicast group number from the specified multicast monitor VLAN.
zte(cfg)#**set igmp snooping timeout** <*100-2147483647*>{**host**|**router**}	This sets multicast member/route timeout.

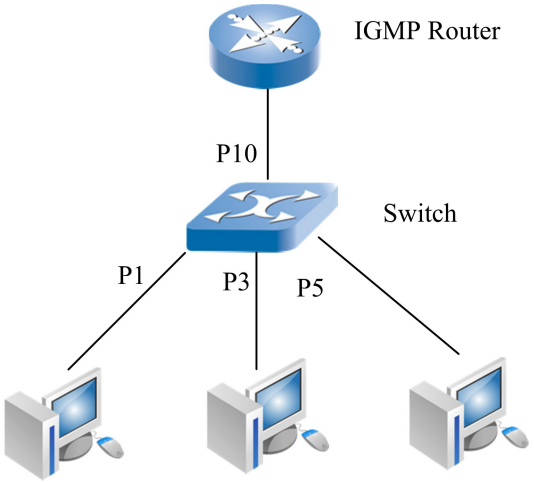
Command	Function
zte(cfg)#**set igmp snooping query-interval** <*10-2147483647*>	This sets the snooping interval. the default value is 1250, which represents 125 seconds. 10 represents 1 second, 20 represents 2 seconds….2147483647 represents 214748364.7 seconds.
zte(cfg)#**set igmp snooping response-interval** <*10-250*>	This sets the snooping response interval. The default value is 100, which represents 10 seconds. 10 represents 1 second, 20 represents 2 seconds….250 represents 25 seconds.
zte(cfg)#**set igmp snooping last-member-query** <*10-250*>	This sets the snooping interval of last member. The default value is 10. 10 represents 1 second, 20 represents 2 seconds….250 represents 25 seconds.
zte(cfg)#**set igmp snooping fastleave** {**enable**|**disable**}	This enables or disables the IGMP fastleave function. The default is **disable**.
zte(cfg)#**set igmp snooping crossvlan** {**enable**|**disable**}	This enables or disables cross-vlan snooping function. The default is **disable**.
zte(cfg)#**set igmp filter** {**enable**|**disable**}	This enables or disables the IGMP filter. The default is **disable**.
zte(cfg)#**set igmp filter add groupip** <*A.B.C.D*> **vlan** <*vlanlist*>	This adds multicast filter group address into the specified multicast monitor VLAN. The parameter **groupip** <*A.B.C.D*>: IP address, the range is from 224.x.x.x to 239.x.x.x except 224.0.0.x.
zte(cfg)#**set igmp filter delete groupip** <*A.B.C.D*> **vlan** <*vlanlist*>	This deletes multicast filter group address from the specified multicast monitor VLAN.

Command	Function
zte(cfg)#**set igmp filter add sourceip** <*A.B.C.D*> **vlan** <*vlanlist*>	This adds the multicast filter source address into the specified multicast monitor VLAN.
zte(cfg)#**set igmp filter delete sourceip** <*A.B.C.D*> **vlan** <*vlanlist*>	This deletes the multicast filter source address from the specified multicast monitor VLAN.
zte(cfg)#**set igmp snooping private-group** <*A.B.C.D*>	This configures the IP address of IGMP private-group packet.
zte(cfg)#**set igmp snooping private-group** {**enable** | **disable**}	This enables or disables the function of IGMP private-group IP packet.
zte(cfg)#**set igmp snooping query version** {**v2**|**v3**}	This sets IGMP snooping query version.
zte(cfg)#**set igmp snooping proxy version** {**v2**|**auto**}	This sets IGMP snooping proxy version.
zte(cfg)#**set igmp snooping v3** {**enable**|**disable**}	This sets IGMP snooping v3 version multicast.
zte(cfg)#**show igmp snooping**	This displays the configuration of IGMP snooping.
zte(cfg)#**show igmp snooping vlan** [<*vlanname*>[**host**|**router**]]	This displays the configuration of IGMP snooping result.
zte(cfg)#**show igmp filter**	This displays the configuration of IGMP filter.
zte(cfg)#**show igmp filter vlan** <*1-4094*>	This displays the multicast snooping results.
zte(cfg)#**show igmp snooping v3 port** <*num*>	This displays the v3 multicast snooping results of the port.
zte(cfg)#**show igmp snooping v3 trunk** <*num*>	This displays the v3 multicast snooping results of the aggregation port.

IGMP Snooping Configuration Example

As shown in Figure 62, ports 1, 3, and 5 are connected to the host. Port 10 is connected to the router. Add port 10, 1, 3, and 5 into VLAN200, User on port 1, 3, and 5 send the multicast join request packet whose multicast address is 230.44.45.167 and 230.44.45.157 respectively. Add multicast filter group address 230.44.45.167 on VLAN200. The IGMP Snooping function and IGMP Filter function are enabled and the snooping results are displayed.

FIGURE 62 NETWORK TOPOLOGY FOR ONE-TO-MANY COMMUNICATION



The detailed configuration is as follows:

```
zte(cfg)#set vlan 200 add port 1, 3, 5, 10 untag
zte(cfg)#set port 1, 3, 5, 10 pvid 200
zte(cfg)#set vlan 200 enable
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 200
zte(cfg)#set igmp filter enable
zte(cfg)#set igmp filter add groupip 230.44.45.167 vlan 200
/*Display the multicast snooping results:*/
zte(cfg)#show igmp snooping vlan
Num  VlanId   Group              Last_Report      PortMember
1     200      230.44.45.157       192.168.1.1       1, 3, 5, 10

zte(cfg)#sho igmp filter
  IGMP Filter: enabled
  Index   FilterIpAddress   Vlan            Port            Type
--------------- --------------- --------------- -------------- ---
  1       230.44.45.167     200            ------          Groupip

zte(cfg)#show igmp filter vlan 200
  Maximal group number: 256
  Current group number: 0
  The filter address list of this vlan:
  Index   FilterIpAddress   Vlan    Type
  ----- ----- ----- ----- ----- ----- ----- ----- ----- -----
  1      230.44.45.167     200    Groupip
```

IPTV Configuration

IPTV Overview

Internet Protocol television (IPTV) is also called Interactive Network TV. IPTV is a method of distributing television content over IP that enables a more customized and interactive user experience. IPTV could allow people who were separated geographically to watch a movie together, while chatting and exchanging files simultaneously. IPTV uses a two-way broadcast signal sent through the provider's backbone network and servers, allowing viewers to select content on demand, and take advantage of other interactive TV options. IPTV can be used through PC or "IP machine box + TV".

Basic Configuration of IPTV

The IPTV configuration covers the following contents.

Command	Function
zte(cfg-nas)#**iptv control** {**enable** | **disable**}	This enables or disables iptv control. The default is disable.
zte(cfg-nas)#**iptv cac-rule**{**enable** | **disable**}	This enables or disables the cac control. The default is disable.
zte(cfg-nas)#**iptv sms-server** <*A.B.C.D*>	This sets the IP address of SMS. The default IP address of SMS is 192.168.0.119.
zte(cfg-nas)#**iptv sms-server-port** <*1025-65535*>	This sets the TCP port of the SMS server. The default TCP port of SMS server is 5115.
zte(cfg-nas)#**show iptv control**	This displays the iptv global configuration.
zte(cfg-nas)#**iptv channel mvlan** <*1-4094*> **groupip** <*A.B.C.D*>[**name** < *channel-name* >[**id** <*channel-id*>]]	This creates the channel. The parameter **groupip** <*group-ip*>: multicast address, 224.0.1.0~239.255.255.255 The parameter **name** < *channel-name* >: 1-32 characters.
zte(cfg-nas)#**clear iptv channel** {**name** <*channel-name*>| **id-list** <*channel-list*>}	This clears a channel.

Command	Function
zte(cfg-nas)#**clear iptv channel all**	This clears all the channels.
zte(cfg-nas)#**iptv channel mvlan** <*vlan-id*> **groupip** <*group-ip*>[**count** <*count-value*>[**prename** <*prename-str*>]]	This creates channels in batch. The parameter **groupip** <*group-ip*>: multicast address, 224.0.1.0~239.255.255.255 The parameter **name** < *channel-name* >: 1-32 characters.
zte(cfg-nas)#**iptv channel name**<*old-name*> **rename** <*new-name*>	This renames a channel. The length of parameter **<***old-name*> and **<***new-name*> are both 1-32 characters.
zte(cfg-nas)#**iptv channel** {**name**<*channel-name*>| **id-list**< *channel-idlist*>}{**view file-name** <*viewfile-name*>|**viewfile-id**< *viewfile-id*>}	This specifies the preview configuration files. **<***channel-name* >:channel-name, 1-32 characters. **<***viewfile-name*>: view file name, 1-60 characters. **<***viewfile-id*>: view file configuration id (0-255).
zte(cfg-nas)#**iptv channel** {**name**<*channel-name*>	**id-list**< *channel-idlist*>}{**enable**	**disable**}	This enables or disables the channel log.
zte(cfg-nas)#**show iptv channel** [**name** <*channel-name*>| **id** <*channel-id*>]	This displays the channel information.
zte(cfg-nas)#**iptv package name** <*package-name*> **channel** {**id-list**<*channel-idlist*>| **name**<*channel-name*>}{**deny**	**order**	**preview**}	This creates multicast package. **<***package-name*>: package name, 1-32 characters. **<***package-id*>: package id, 0~127, package-id and package-name are unique. The system distributes an id value when package-id is not chose.
zte(cfg-nas)#**clear iptv package** {**name**<*package-name*>| **id-list**< *package-idlist* >}	This deletes the package.
zte(cfg-nas)#**clear iptv package all**	This deletes all the packages.

Command	Function
zte(cfg-nas)#**iptv package name** <*package-name*> **channel** {**id-list**<*channel-idlist*>| **name**<*channel-name*>}[**deny** | **permit** | **preview**]	This adds the channel to the multicast package and sets multicast authority.
zte(cfg-nas)#**show iptv package** [**name**<*package-name*>| **id**<*package-id*>]	This displays the multicast package
zte(cfg-nas)#**iptv prv** {**enable** | **disable**}	This enables/disables iptv preview. The default is disable.
zte(cfg-nas)#**iptv prv reset**	This resets iptv preview timer to 0.
zte(cfg-nas)#**iptv prv autoreset-time** <*HH:MM:SS*>	This sets iptv preview autoreset-time. The default value is 00:00:00.
zte(cfg-nas)#**iptv prv recognition-time** <*1-65534*>	This sets iptv preview recognition-time. The default value is 4 seconds.
zte(cfg-nas)#**iptv prv overcount-cdr** {**enable** | **disable**}	This enables or disables iptv preview overcount-cdr function. The default is disable.
zte(cfg-nas)#**show iptv prv**	This displays iptv preview global configuration.
zte(cfg-nas)#**iptv view-profile name** < *viewfile-name*>[**id** <*view-profile-id*>]	This creates iptv preview configuration files. The parameter **name** < *viewfile-name*> :1-60 characters.
zte(cfg-nas)#**clear iptv view-profile**{ **name**<*viewfile-name*>| **id-list**<*view-profile-idlist* >}	This deletes iptv preview configuration files.
zte(cfg-nas)#**clear iptv view-profile all**	This deletes all the iptv preview configuration files.
zte(cfg-nas)#**iptv view-profile name** <*viewfile-name*> **count** <*view-count*>	This sets the maximum preview times. The parameter **name** <*viewfile-name*>: 1-60 characters The parameter **count** <*view-count*> : maximum preview times, 1~200 and the default is 3.

Command	Function
zte(cfg-nas)#**iptv view-profile name** <*viewfile-name*> **duration** <*view-duration*>	This sets the single maximum preview time. The parameter **duration** <*view-duration*>: single maximum preview time (1-65535). The default is 120s.
zte(cfg-nas)#**iptv view-profile name** <*viewfile-name*> **blackout** < *view-interval* >	This sets the minimum preview time interval. The parameter **blackout** < *view-interval* > : minimum preview time interval 1-65535, the default value is 60s.
zte(cfg-nas)#**show iptv view-profile** [**name**<*viewfile-name*>| **id** <*view-profile-id*>]	This displays the preview configuration files.
zte(cfg-nas)#**iptv cdr** {**enable** | **disable**}	This enables or disables iptv cdr record function.
zte(cfg-nas)#**iptv cdr max-records** <*cdr-size*>	This sets cdr maximum record items. The default is 1000.
zte(cfg-nas)#**iptv cdr report**	This reports cdr manually.
zte(cfg-nas)#**iptv cdr report-interval** <*report-interval*>	This sets the time interval for CDR report. The parameter **report-interval** <*report-interval*>: the report interval 1-65535. The default value is 300 seconds.
zte(cfg-nas)#**iptv cdr report -threshold** <*1-32*>	This configures the number of CDR records for reporting every time. The default value is 10.
zte(cfg-nas)#**iptv cdr create-period** <*period*>	This configures the interval for creating CDR record when user watches programs for long time. The parameter **create-period** <*period*>: the interval for creating CDR record when user watches programs for long time(1-65535). The default value 3600s.

Command	Function
zte(cfg-nas)#**iptv cdr deny-right** {**enable** | **disable**}	This enables or disables cdr record function when the access authorization is deny. The default is disable.
zte(cfg-nas)#**iptv cdr prv-right** {**enable** | **disable**}	This enables or disables cdr record function when the access authorization is preview. The default is disable.
zte(cfg-nas)#**iptv cdr warning-threshold** <*threshold value*>	This sets the warning-threshold of CDR cache pool. The default value is 50%.
zte(cfg-nas)#**show iptv cdr**	This displays the configured CDR attribute.
zte(cfg-nas)#**iptv port** <*portlist*>[**vlan** <*vlan-id*>] **service** {**start** | **pause** | **resume** | **remove**}	This sets the current service state of user.
zte(cfg-nas)#**iptv port** <*portlist*>[**vlan** <*vlan-id*>] **control-mode** {**package** | **channel**}	This sets multicast control-mode of user.
zte(cfg-nas)#**iptv port** <*portlist*>[**vlan** <*vlan-id*>] **package**{**name**<*package-name*>| **id** <*package-id*>}	This distributes package to users.
zte(cfg-nas)#**clear iptv port** <*portlist*>[**vlan** <*vlan-id*>] **package**{ **name** <*package-name*>| **id** <*package-id*>}	This deletes the distributed package.
zte(cfg-nas)#**iptv port** <*portlist*>[**vlan** <*vlan-id*>] **channel** {**name** <*channel-name*>| **id-list** <*channel-idlist*>}{**deny** | **order** | **preview** | **query**}	This configures channel access authorization of user port.
zte(cfg-nas)#**iptv port** <*portlist*>[**vlan**<*vlan-id*>] **cdr** {**enable** | **disable**}	This configures whether the user opens CDR record function. The default setting is enabled.
zte(cfg-nas)#**iptv port** <*portlist*>[**vlan** <*vlan-id*>] **mac-base** {**enable** | **disable**}	This configures whether the user opens the mac-based management. The default is disabled.
zte(cfg-nas)#**show iptv rule** [**port** <*portid*>[**vlan** <*1-4094*>[**channel** | **package**]| **channel** | **package**]]	This displays the information of iptv rule.

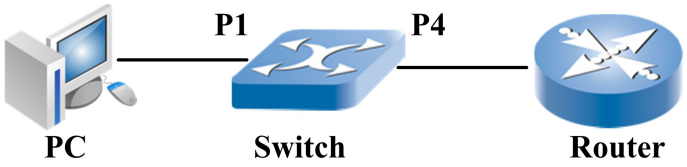
Command	Function
zte(cfg-nas)#**show iptv client** [{**channel** <*channel-id*>| **index** <*index-id*>| **mac** <*HH.HH.HH.HH.HH.HH*>| **port** <*portid*>| **vlan** <*vlanid*>}]	This displays the information of iptv client.
zte(cfg-nas)#**clear iptv client** [**index** <*index-id*>| **mac** <*HH.HH.HH.HH.HH.HH*>| **port** <*port-id*>[**vlan**<*1-4094*>]]	This deletes the information of iptv client.

IPTV Configuration Example

1. Example 1

   As shown in Figure 63, port 1 connects with the user and it is the order user of channel 225.1.1.1. The user vlan is 100. The multicast vlan is 4000. Router sends data stream of multicast group 225.1.1.1. PC sends request for entering into channel 225.1.1.1.

FIGURE 63 IPTV CONFIGURATION EXAMPLE



Configuration of switch:

i. Configure vlan

```
zte(cfg)#set vlan 100 add port 1
zte(cfg)#set vlan 4000 add port 1, 4
zte(cfg)#set vlan 100, 4000 enable
zte(cfg)#set port 1 pvid 100
zte(cfg)#set port 4 pvid 4000
/*IGMP Snooping*/
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 100, 4000
zte(cfg)#set igmp snooping fastleave enable
```

ii. Configure IPTV

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control enable
zte(cfg-nas)#iptv cac-rule enable
```

iii. Configure rules on port

```
zte(cfg-nas)#iptv channel mvlan 4000 group 225.1.1.1 name CCTV1  id 1
zte(cfg-nas)#iptv port 1 service start
zte(cfg-nas)#iptv port 1 control-mode channel
zte(cfg-nas)#iptv port 1 channel id-list 1 order
```

iv. View the configuration

```
zte(cfg-nas)#show iptv rule
  MaxRuleNum:64
  CurRuleNum:1
  HisRuleNum:1
Id  Port Vlan  Mbase  Mode Service Cdr Order Prview Query PkgNum
  --  ---- ----  ----- ------- ------- -------- ------ ------ ----- -----
```

```
1    1      false  channel   in   disabled  1     0      0         0
/*view the user online state when the user is online*/
zte(cfg-nas)#show igmp snooping vlan
  Num  VlanId    Group           Last_Report    PortMember
  ---     -------   --------------        --------------- -------
  1      4000    225.1.1.1          25.1.1.1             1
zte(cfg)#show iptv client index 0
  Index    :0
  Rule     :1                          Vlan  :100
  Port     :1                          ChNum :1
  Mac     :00.00.02.00.00.11             Ip  :25.1.1.1

  Channel  UserType    MultiAddress      ElapsedTime
  ---------    ----------      -----------       --------------
  1          order       225.1.1.1        0:0:0:26
```

2. Example 2

   As shown in Figure 63, port 1 connects with the user and it is the preview user of channel 225.1.1.1. The maximum preview time is 20 seconds, the interval is at least 10 seconds and the maximum preview time is 2. The user vlan is 100. The multicast vlan is 4000. Router sends data stream of multicast group 225.1.1.1. PC sends request for entering into channel 225.1.1.1.

   Configuration of switch:

   i. Configure VLAN

```
zte(cfg)#set vlan 100 add port 1
zte(cfg)#set vlan 4000 add port 1, 4
zte(cfg)#set vlan 100, 4000 enable
zte(cfg)#set port 1 pvid 100
zte(cfg)#set port 4 pvid 4000
/*IGMP Snooping*/
zte(cfg)#set igmp snooping enable
zte(cfg)#set igmp snooping add vlan 100, 4000
zte(cfg)#set igmp snooping fastleave enable
```

   ii. Configure IPTV

```
zte(cfg)#config nas
zte(cfg-nas)#iptv control enable
zte(cfg-nas)#iptv cac-rule enable
zte(cfg-nas)#iptv prv enable
```

   iii. Configure rules on the port

```
zte(cfg-nas)#iptv channel mvlan 4000 group 225.1.1.1 name CCTV1  id 1
zte(cfg-nas)#iptv port 1 service start
zte(cfg-nas)#iptv port 1 control-mode channel
zte(cfg-nas)#iptv port 1 channel id 1 preview
```

   iv. Configure preview template

```
zte(cfg-nas)#iptv view-profile name VPF1.PRF
zte(cfg-nas)#iptv view-profile name VPF1.PRF count 2
zte(cfg-nas)#iptv view-profile name VPF1.PRF blackout 10
zte(cfg-nas)#iptv view-profile name VPF1.PRF duration20
zte(cfg-nas)# iptv channel id 1 viewfile-name VPF1.PRF
```

   v. View the configuration

```
/*view the preview template*/
zte(cfg-nas)#show iptv view-profile name vpf1
  ViewProfile Id     :1
  MaxprvCount     :2
  MaxprvDuration   :20
  BlackoutInterval   :10

/*view the user online condition when the user is online*/
zte(cfg-nas)#show iptv client index 0
  Index    :0
  Rule     :1                          Vlan  :100
```

```
Port     :1                          ChNum :1
Mac     :00.00.02.00.00.11             Ip    :25.1.1.1

Channel  UserType    MultiAddress      ElapsedTime
-------      ----------    ----------------      --------------
1        preview      225.1.1.1         0:0:0:12
```

DHCP CLIENT Configuration

DHCP CLIENT Overview

ZXR10 2920/2928/2952/2936-FI not only supports the static IP address configured on layer 3 interface but also supports getting dynamic IP address from DHCP server, which implements the normal communication based on layer 3.

At this time, switch takes as DHCP client, the valid use time of the applying dynamic address is called leased time. Before the leased time expires, the host should request continuous leasing from the server, and the address can be used continuously only after the server accepts the request.

The process of application and lease needn't manual intervention, the necessary configuration can be done before use.

Basic Configuration of DHCP CLIENT

1. Global Configuration

Command	Function
`zte(cfg)#`**set dhcp client** {**enable**|**disable**}	This enables/disables DHCP CLIENT at global configuration mode.
`zte(cfg)#`**set dhcp client broadcast-flag** {**enable**|**disable**}	This sets DHCP CLIENT broadcast-flag.

2. Layer 3 Interface Configuration

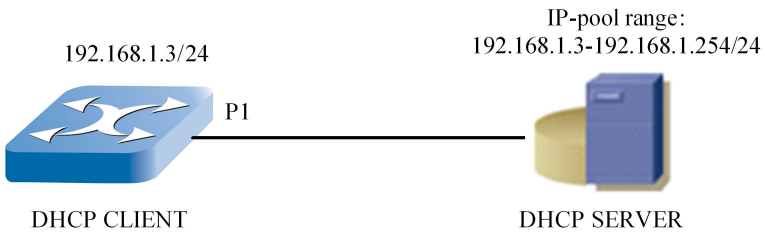
   Enter layer 3 configuration mode by using the command config router before configuring DHCP CLIENT on layer 3 interface mode.

Command	Function
zte(cfg-router)#**set ipport** *<0-63>* **ipaddress dhcp**	This configures the mode that layer 3 interface getting address as DHCP.
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client class-id characters** *<string>*	This configures device type.
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client class-id hex-numbers** *<hex-string>*	
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client client-id mac**	This sets client ID which is the unique ID of client.
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client hostname** *<string>*	This sets client name.
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client lease** *<day><hour><minute>*	This sets the lease that client suggests, the format can be infinite or day/hour/minute.
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client lease infinite**	
zte(cfg-router)#**set ipport** *<0-63>* **dhcp client request** { **dns-server**| **domain-name**| **router**| **static-route**| **tftp-server-name** }	This sets client request items, the server fill in response contents according to request items.
zte(cfg)#**clear ipport** *<0-63>* **dhcp client class-id**	This clears DHCP CLIENT parameters.
zte(cfg)#**clear ipport** *<0-63>* **dhcp client client-id**	
zte(cfg)#**clear ipport** *<0-63>* **dhcp client hostname**	
zte(cfg)#**clear ipport** *<0-63>* **dhcp client lease**	
zte(cfg)#**clear ipport** *<0-63>* **dhcp client request**	

DHCP CLIENT Configuration Example

The figure is shown as Figure 64.

FIGURE 64 DHCP CLIENT CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#set vlan 100 enable
zte(cfg)#set vlan 100 add port 1 untag
zte(cfg)#set port 1 pvid 100
zte(cfg)#set dhcp client enable
zte(cfg)#config route
zte(cfg-router)#set ipport 0 ipaddress dhcp
zte(cfg-router)#set ipport 0 vlan 100
zte(cfg-router)#set ipport 0 enable
zte(cfg-router)#show ipport
IpPort  Status IpAddress   Mask  MacAddress  VlanId  IpMode
------ ------  ---------   ----- ---------------   ---
  0    up  192.168.1.3   255.255.255.0  00.0d.1c.52.22.22 100 dhcp
zte(cfg-router)#show ipport 0
  Status    : up          IpAddress : 192.168.1.3
  VlanId    : 100         Mask    : 255.255.255.0
  ArpProxy : disabled      MacAddress: 00.0d.1c.52.22.22
  Timeout   : 600(s)       IpMode    : dhcp
  En/Disable: enabled

Dhcp client configuration as follows:
  Class-id     : -
  Client-id    : -
  Hostname   : -
  Lease       :-
  Clear request: -
```

DHCP Snooping/Option82 Configuration

DHCP Snooping/Option82 Overview

The DHCP (Dynamic Host Configuration Protocol) enables the host to apply dynamic addresses from server.

DHCP snooping function prevents bogus DHCP server from being laid in network, and in this case, the port connecting to DHCP server must be set to trusted port. What's more, dynamic ARP inspection technology can be used together to prevent illegal IP and MAC address binding, thus ensuring normal assignment of IP addresses by DHCP server. DHCP Snooping and Option82 are designed to solve these safety problems. DHCP Snooping, namely DHCP packet filtering, is to detect legality of DHCP packets based on some special rules and filter illegal packets. Use Option82 tech-

nique to provide more additional information, and then strengthen the network safety ability.

Basic Configuration of DHCP Snooping/Option82

Configure the following commands to support Snooping and Option82 functions.

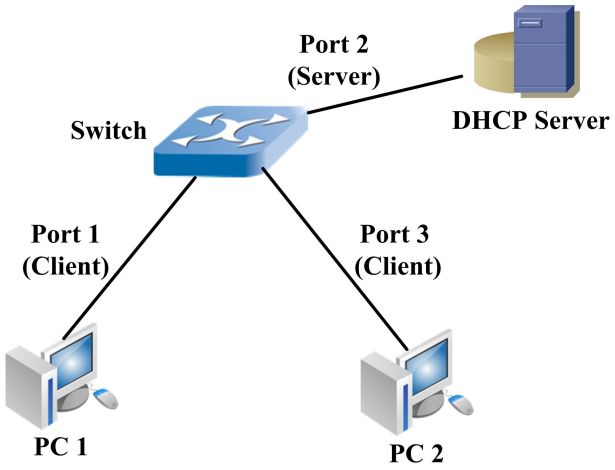
Command	Function
zte(cfg)#**clear dhcp snp-bind-entry** {**all** | **port** <*portname*>| **mac** <*HH.HH.HH.HH.HH.HH*>}	This clears DHCP Snooping dynamic binding table.
zte(cfg)#**clear dhcp option82 ani**	This clears the switch accessing node identifier.
zte(cfg)#**set dhcp snooping-and-option82** {**enable** | **disable**}	This enables/disables DHCP, the default is disable.
zte(cfg)#**set dhcp port** <*portname*>{**server** | **cascade** | **client**}	This configures DHCP attribute of port. There are three kinds of attributes of the port: server port, cascade port and client port. Only server port is the trusted port. If the switch is connected with DHCP relay device and the uplink port is setting as trunk, then the uplink port attribute must be trusted. The trusted port receives and transmits DHCP Offer normally, but the untrusted port discards DHCP Offer packet. This ensures that the client terminal can obtain IP address from the legal DHCP server.
zte(cfg)#**set dhcp snooping** {**add** | **delete**}{**port** <*portlist*>|**trunk**<*trunklist*>}	This enables/disables DHCP Snooping function based on port.
zte(cfg)#**set dhcp option82** {**add** | **delete**}{**port** <*portlist*>|**trunk**<*trunklist*>}	This enables/disables DHCP Option82 function based on port.

Command	Function
zte(cfg)#**set dhcp option82 ani** <*string*>	This configures access node identifier. The parameter < string > can not be more than 50 characters.
zte(cfg)#**set dhcp option82 sub-option port** <*portname*>{**circuit-ID** {**on** {**cisco** | **china-tel** | **dsl-forum**}| **off**}| **subscriber-ID** {**on** <*string*> **off**}| **reserve** {**on tag** <*1-255*> **value** <*string*>| **off**}}	This sets DHCP Option82 sub-option based on port. circuit-ID: If set circuit-id as CHINA-TEL or DSL-Forum, the switch access node must be set at first.
zte(cfg)#**show dhcp**	This displays DHCP global information.
zte(cfg)#**show dhcp snooping**	This displays DHCP Snooping configurations.
zte(cfg)#**show dhcp snooping binding** [**port** <*portname*>]	This displays information of DHCP Snooping dynamic binding table.
zte(cfg)#**show dhcp option82**	This displays information of DHCP Option82 configuration information.
zte(cfg)#**show dhcp option82 ani**	This displays the information of DHCP Option82 access node identifier.
zte(cfg)#**show dhcp option82 port** <*portname*>	This displays DHCP Option82 configuration information based on port.

DHCP Snooping/Option82 Configuration Example

As shown in Figure 65, PC can get IP address from specified DHCP server and prevent other illegal DHCP servers from affecting hosts in the network.

FIGURE 65 DHCP SNOOPING CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#set dhcp en
zte(cfg)#set dhcp port 1 client
zte(cfg)#set dhcp port 2 server
zte(cfg)#set dhcp snooping add port 1-2
zte(cfg)#set dhcp ip-source-guard add port 1
zte(cfg)#show dhcp
  DHCP is enabled.
  PortId    PortType    Snooping    Option82
  ------      --------      --------      --------
  1         Client      Enabled     Disabled
  2         Server      Enabled     Disabled
3         Client      Disabled    Disabled
  4         Client      Disabled    Disabled
  5         Client      Disabled    Disabled
  6         Client      Disabled    Disabled
zte(cfg)#show dhcp snooping
  DHCP snooping is enabled on the following port(s):
  PortId    PortType
  ------    --------
  1         Client
  2         Server
zte(cfg)#show dhcp ip-source-guard
  Ip source guard is configured on the following port(s):
```

VBAS Configuration

VBAS Conifguration Overview

VBAS is not physical equipment but a protocol standard, which is developed by Guangdong Institute of China Telecom. VBAS is to solve the problem of wide-band user identifier. When BAS gets user identifier by inquiring corresponding relationship between MAC of users dialing to the switch and port, then sends user name, password and identifier information to RADIUS, it can judge the position of the user.

Layer 2 communication mode is implemented between BAS and switches, that is, information query and response data packets

of VBAS are encapsulated into Ethernet data frames of layer 2 directly, and use protocol number 0x8200 to identify.

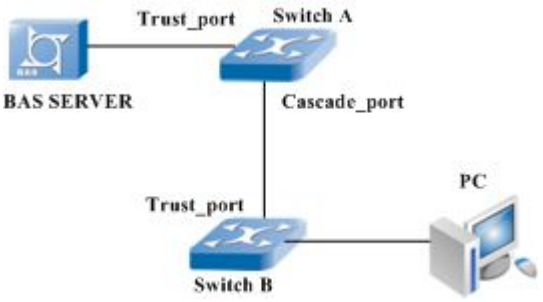
The VBAS function is supported in ZXR10 2609-EI/2818S-EI/2826S-EI.

Caution:

Only trust ports can receive VBAS packets and VBAS response packets only can be sent from trust ports.

Port connecting to user network is called cascade port and port connecting to BAS server is called trust port. Typical network of VBAS is shown in Figure 66.

FIGURE 66 TYPICAL NETWORK OF VBAS



Basic Configuration of VBAS

To configure VBAS, perform the following steps.

Command	Function
zte(cfg)#**set vbas** {**enable**|**disable**}	This enables or disables global VBAS function. VBAS function is disabled by default.
zte(cfg)#**set vbas trust-port** <*portlist*>{**enable**|**disable**}	This enables or disables trust port VBAS function. The port is untrusted by default.
zte(cfg)#**set vbas cascade-port** <*portlist*>{**enable**|**disable**}	This enables or disables cascade port VBAS function. By default, the port is in noncasecade state.
zte(cfg)#**show vbas**	This displays VBAS configuration.

VBAS Configuration Example

As shown in "VBAS Typical Network", this example describes how to set trust port of switch A as port 1, cascade port as port 2, trust port of switch B as port 1.

Configuration of switch A:

```
zte(cfg)#set vbas en
zte(cfg)#set vbas trust_port 1 en
zte(cfg)#set vbas cascade_port 2 en
zte(cfg)#show vbas
  vbas: enabled
  trust port   : 1
  cascade port : 2
```

Configuration of switch B:

```
zte(cfg)#set vbas enable
zte(cfg)#set vbas trust-port 1 enable
zte(cfg)#show vbas
  vbas: enabled
  trust port   : 1
  cascade port : none
```

EPON

EPON Overview

The Development of PON

With the development of network technology, the speed of backbone network and LAN is improved greatly. The last one mile is the bridge between the network and family user, and now it is the bottleneck to limit the network development.

The former accessing technologies such as T1/E1 or SONET/SDH cost too much, and optical accessing technologies such as Cable Modem requires high cost of network constructing, wireless accessing technology is restricted by environment and security and is not easy to launch.

Passive Optical Network (PON) is an accessing technology, which guarantees the user to obtain enough accessing bandwidth and controls the network construction cost effectively.

PON Overview

Optical access includes two types:

- Active Optical Network (AON)
- Passive Optical Network (PON)

PON is a pure physical media network, the active device is not required between the central office end and terminal, which effectively avoids electromagnetic interference of peripheral equipments, reduces the failure rate of lines and devices, improves the system reliability and saves the maintenance cost.

PON is transparent to services, so it is applicable to process the signal with many modes and rates. APON/BPON, GPON

and EPON/GEPON are PON-based technologies. They adopt the different L2 technologies.

EPON Overview

Ethernet in the First Mile Alliance (EFMA) brought forward EPON in 2001, which replaces ATM with Ethernet network on layer 2, and IEEE 802.3ah working group standardized EPON. IEEE 802.3 EFM working group released IEEE 802.3ah as EPON standard in June, 2004 (This standard was merged into IEEE 802.3-2005 standard) to solve the problem of "the last one mile".

EPON is Ethernet network carrying on PON network, which supports 1.25Gbps symmetric rate. It is easy to deploy and maintain. Meanwhile, EPON inherits simplicity and high efficiency from Ethernet network. It is very suitable for wide-band access of IP service to combine Ethernet and PON technologies together.

EPON needn't complex protocol and optical signal can be correctly transmitted between central office and terminal. EPON applies mature full duplex Ethernet technology and TDM(Time Division Multiplex and Multiplexer). ONU sends data packet in its time slot so it doesn't have conflict with other ONUs, which makes the best use of the bandwidth.

EPON Characteristics

- All bearer devices in EPON network are passive, so the power network is not required.
- EPON adopts wavelength division multiplexing technology. The uplink and downlink flow are transmitted on an optical fiber, which saves a lot of fiber.
- EPON works on physical and logical link layer. It is totally transparent to the high level services and protocol.
- EPON is point to multi-point access method, which saves the port numbers on convergence side.

EPON Related Concepts

- OLT: Optical Line Terminal. The convergence node on the direction of uplink. It is the optical line terminal on central office end.
- ONU: Optical Network Unit. It is the access node of optical network unit on subscriber side.

EPON Function of ZXR10 2900

ZXR10 2920 and ZXR10 2928 become ONU after loading PON function daughter card. PON function daughter card is shown as "RS-2800-1GE-SFF". When the uplink optical port of PON daughter card connects with OLT on central office side, switch accesses EPON network system.

EPON network system has the ability to carry Ethernet/IP service and can support voice service, TDM service and CATV service. ONU supports OLT remotely manages it by extended OAM.

Note:

There is big difference between ONU and switch for the function took by ZXR10 2920 and ZXR10 2928. Therefore ZXR10 2920 and ZXR10 2928 can't act as ONU and traditional switch at the same time.

Basic Configuration of EPON

To configure EPON, perform the following steps.

1. To restart PON subboard, use the following command.

Command	Function
zte(cfg)#**set epon reset**	This restarts PON subboard.

2. To enable or disable the port on PON subboard, use the following command.

Command	Function
zte(cfg)#**set epon port** {**enable** | **disable**}	This enables or disables the port on PON subboard.

3. To configure the schedule mode of PON subboard, use the following command.

Command	Function
zte(cfg)#**set epon schedule** {**SP** | **WRR** *<1-8>*}	This configures the schedule mode of PON subboard.

4. To show link status of PON subboard, use the following command.

Command	Function
zte(cfg)#**show epon**	This shows the status of PON subboard.

5. To show PON subboard firmware information and EPON system configuration information, use the following command.

Command	Function
zte(cfg)#**show epon firmware-infor**	This shows PON subboard firmware information and EPON system configuration information.

6. To show port information of PON subboard, use the following command.

Command	Function
zte(cfg)#**show epon port**	This shows the port information of PON subboard.

7. To show OAM information of PON subboard port, use the following command.

Command	Function
zte(cfg)#**show epon port oam**	This shows OAM information of PON subboard port.

8. To show PON schedule information, use the following command.

Command	Function
zte(cfg)#**show epon schedule**	This shows PON schedule information.

EPON Service Switch Configuration

When ZXR10 29290/2928 acts as ONU device, a part of services will be changed. The following contents describe the differences between added with PON daughter card or without PON daughter card.

1. Port configuration

Command	Function
zte(cfg)#**set port** <*portlist*> **vlan-mode** {**transparent** | **tag** | **translation**}	This configures the function mode of port on VLAN.

transparent: transparent mode.

tag: tag forwarding mode.

translation: VLAN translation mode.

This command is valid only after ZXR10 2920/2928 added with PON daughter card and acting as ONU device.

Caution:

Although ZXR10 2952 and ZXR10 2936-FI provide this command, but the two types can't provide the function of adding with PON daughter card. Therefore this command is invalid for ZXR10 2952 and ZXR10 2936-FI.

2. VLAN Initialization Configuration

Command	Function
`zte(cfg)#`**show vlan**	This shows all VLANs information on switch.

After the switch added with PON daughter card, the switch acts as ONU device, all VLANs (1-4094) are enabled. The port 1-19 are added into VLAN 1 with UNTAG, and they are added into VLAN 2-4094 with TAG. Use the show vlan command to show all Vlans information.

When the switch does not add with PON daughter card, only VLAN 1 is enabled . Port 1-18 are added into VLAN 1 with UNTAG. Use the **show vlan** command to show the information of VLAN 1.

Example:

The following example shows that daughter card is added with ZXR10 2920/2928.

```
zte(cfg)#show vlan
  VlanType: 802.1q vlan

  VlanId  : 1     VlanStatus: enabled
  VlanName:
  VlanMode: Static
  Tagged ports    :
  Untagged ports  : 1-19
  Untagged trunks : 1-15
  Forbidden ports :

  VlanId  : 2     VlanStatus: enabled
  VlanName:
  VlanMode: Static
  Tagged ports    : 1-19
  Tagged trunks   : 1-15
  Untagged ports  :
  Forbidden ports :

  VlanId  : 3     VlanStatus: enabled
  VlanName:
  VlanMode: Static
  Tagged ports    : 1-19
  Tagged trunks   : 1-15
  Untagged ports  :
  Forbidden ports :

  VlanId  : 4     VlanStatus: enabled
  VlanName:
  VlanMode: Static
  Tagged ports    : 1-19
  Tagged trunks   : 1-15
  Untagged ports  :
```

```
  Forbidden ports :
… …/*the display of vlan5-vlan4093 is omitted*/
  VlanId  : 4094  VlanStatus: enabled
  VlanName:
  VlanMode: Static
  Tagged ports    : 1-19
  Tagged trunks   : 1-15
  Untagged ports  :
  Forbidden ports :
```

The following example shows that daughter card is not added with ZXR10 2920/2928.

```
zte(cfg)#show vlan
  VlanType: 802.1q vlan
  VlanId  : 1     VlanStatus: enabled
  VlanName:
  VlanMode: Static
  Tagged ports    :
  Untagged ports  : 1-18
  Untagged trunks : 1-15
  Forbidden ports :
  Total Vlans: 1
```

3. VLAN Translation

Command	Function
`zte(cfg)#`**set vlan-translation ingress-port** <*feport-id*> **ingress-vlan** <*vlan-list*> **egress-port** <*geport-id*> **egress-vlan** <*vlan-list*>	This configures VLAN translation function and the related functional port and VLAN.

After ZXR10 2920/2928 adds with PON daughter card, the translation port will discard the TAG packet without translation rule.

When ZXR10 2920/2928 doesn't add with PON daughter card, the translation port will forwards all packets and not discard any packet.

4. IGMP Snooping Function

After ZXR10 2920/2928 adding with PON daughter card, add port-based multicast control on the basis of vlan-based multicast control.

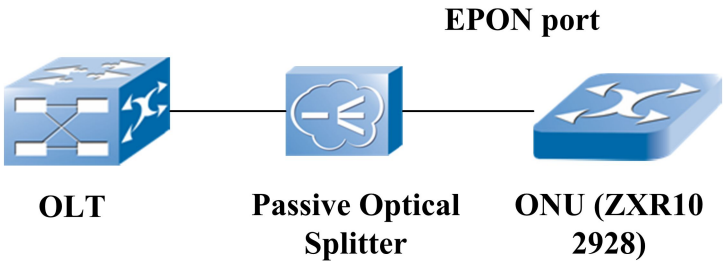
EPON Configuration Example

Example Description

This example describes how to distribute service to ONU by OLT device, and how to view the service configuration information on ONU device.

Network Figure and Description

FIGURE 67 EPON CONFIGURATION EXAMPLE



ZXR10 2928 adds with PON daughter card and connects with optical splitter through the optical port on PON daughter card. The optical splitter connects with OLT device.

Configuration Procedure

1. Configure service of ONUZXR10 2928 on OLT.
2. Check service configuration on ONU.

Configuration Process

The following ONU configurations are performed by OLT.

1. Add ONU into VLAN300. Configure port 1 of ONU to adopt VLAN transparent transmission mode on OLT.
2. Configure port 2 of ONU to adopt TAG mode, the priority is the default value, VID is 100.
3. Configure port 3 of ONU to adopt VLAN translation mode, the default vlan is VLAN100.
4. Create translation rule. Translate the flow of VLAN1000 to VLAN 200.
5. Enable the IGMP Snooping function to monitor VLAN1000.

View the above configurations on ONU device.

```
zte(cfg)#show port 1 vlan
  PortId  : 1
  Tagged in vlan   : 2-999,1001-4094
  Untagged in vlan : 1
zte(cfg)#show port 1 vlan-mode
Port 1 Vlan-mode:Transparent-mode
/*The transparent transmission mode of port 1 has been valid.*/
zte(cfg)#show port 2 vlan-mode
Port 2 Vlan-mode:Tag-mode   Tag value: 100
/*The configuration of port 2 is valid.*/

zte(cfg)#show port 3 vlan-mode
Port 3 Vlan-mode:Translation-mode
/*The configuration of port 3 is valid.*/
zte(cfg)#show port 3
  PortId     : 3              MediaType : 100BaseT
  PortParams:
    PortEnable     : enabled   PortAutoNeg    : enabled
    DefaultVlanId  : 100       FlowControl    : enabled
/*the default vlan is vlan100.*/
    Multicastfilter: disabled  Security       : disabled
    SpeedAdvertise : MaxSpeed  Mdix           : auto
    PortMacLimit   : disabled  UnknownFilter  : disabled
    MacLearning    : enabled       Accept-Frame   : untag-frame
    FixMac         : disabled      FixMode        : none
    RecoverTime    : none
    PortVlanJump   : disabled
  PortStatus:
    PortClass      : 802.3         Link           : down
    Duplex         : half          Speed          : 10Mbps
```

```
zte(cfg)#show vlan-translation
  ingress port:  3   egress port: 19      state: enable
  ingress vlan list: 1000
  egress vlan list : 200 /*VLAN translation rule is valid.*/

zte(cfg)#show igmp snooping
  IGMP snooping: enabled              RouterTimeout: 2600
  FastLeave    : enabled              HostTimeout  : 2600
  QueryInterval: 1250
  CrossVlan snooping: disabled
  ResponseQueryInterval  : 100
  LastMemberQueryInterval: 10
  Snooping VlanId: 1000  /*multicast configuration is valid, snoop VLAN 1000*/
  Querying VlanId: none
  IGMPv3 Snooping: disabled
  Proxy Version: auto
  Query Version: v2
  Private Group: disable
  Private Group Ip: none
  Multicast forwarding all ports!
```

Upgrading PON Daughter Card

Short Description

This following content describes how to upgrade PON daughter card on ZXR10 2920/2928.

Prerequisite

The main system version file kernel.z has been updated on ZXR10 2920/2928. For detailed updating steps, refer to Software Version Upgrade.

Caution:

PON daughter card version file only applies to ZXR10 2920/2928.

Steps

1. Enter into file system configuration mode, delete the old version file from FLASH with **remove** command. The two PON daughter card version files have longer file name, their file extension name are blob and dat respectively, such as:
   - iros_onu_oob_asic_rom_big-02.00.04-1216201110.blob PON daughter card version file
   - eeprom-onu-3d.up.noreset.ctrlvlan0.igmp0.dat PON daughter card configuration file
2. Download the above version files from TFTP server to FLASH with **tftp** command.
3. Upgrade blob file with **update image** command.

   The command format:

   ```
   zte(cfg-tffs)#update image *.blob
   ```

   "*" represents the file name
4. Upgrade dat file with **updateEpon config** command.

   ```
   zte(cfg-tffs)#updateEpon config *.dat
   ```

   "*" represents the file name

5. Restart the switch. After the switch restarts, view the running version to confirm whether the upgrade is successful.

Tip:

The two daughter card file names can be modified into simpler names and then implement upgrade, which simplifies the complex operation of inputting the filename.

Result:

- After *.blob file upgrades successfully, the switch prompts as follows:

```
Update epon image success !
```

- After *.dat file upgrading successfully, the switch prompts as follows:

```
Epon update config success!
```

Example

```
This example describes how to upgrade PON daughter card on ZXR10 2920.
zte(cfg)#conf t
zte(cfg-tffs)#ls
  kernel.z                                          1,798,966 bytes
  snmpboots.v3                                         35 bytes
  epon.txt                                              0 bytes
  eeprom-onu-3d.up.noreset.ctrlvlan0.igmp0.dat            128 bytes
  iros_onu_oob_asic_rom_big-02.00.04-1216201110.blob  293,880 bytes
  startcfg.txt                                        1,015 bytes
  06.dat                                                128 bytes
                    475,136 bytes free

zte(cfg-tffs)#remove iros_onu_oob_asic_rom_big-02.00.04-1216201110.blob
  Sure to remove ? [Yes|No]:y

zte(cfg-tffs)#remove eeprom-onu-3d.up.noreset.ctrlvlan0.igmp0.dat
  Sure to remove ? [Yes|No]:y

zte(cfg-tffs)#tftp 192.168.20.159 down
iros_onu_oob_asic_rom_big-02.00.04-1216201110.blob
.....................................................
  315,844 bytes downloaded

zte(cfg-tffs)#tftp 192.168.20.159 down
eeprom-onu-3d.up.noreset.ctrlvlan0.igmp0.dat
.
  128 bytes downloaded

zte(cfg-tffs)#update image
iros_onu_oob_asic_rom_big-02.00.04-1216201110.blob
.................................................
THU JUL 01 00:11:54 2004 Pon hello process status : DISCONNECTED

THU JUL 01 00:11:54 2004 Port : 19 linkdown

THU JUL 01 00:12:29 2004 Port : 19 linkup
Update epon image success !
THU JUL 01 00:12:34 2004 Pon hello process status : CONNECTED

zte(cfg-tffs)#updateEpon config eeprom-onu-3d.up.noreset.ctrlvlan0.igmp0.dat
Epon update config success!
zte(cfg-tffs)#exit
zte(cfg)#reboot
  Sure to reboot ? [Yes|No]:y
zte(cfg)#system start……
sdram initialized
initializing flash
flash initialized
```

ACL Configuration

ACL Overview

An Access Control List (ACL) is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACL's to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. It tests packets against the conditions in an access list one by one. The first match determines whether the switch accepts or rejects the packets because the switch stops testing conditions after the first match. The order of conditions in the list is critical. If no conditions match, the switch rejects the packets. If there are no restrictions, the switch forwards the packet. otherwise, the switch drops the packet.

ZXR10 2920/2928/2952/2936-FI supports the following functions.

1. ZXR10 2920/2928/2952/2936-FI provides two binding types including physical port and Trunk Groups. When a physical port is added into a Trunk Groups and has been bounded an ACL, current bound will be released first, otherwise, a false message will return. When ACL is applied to Trunk Groups, physical port will be bound with ACL automatically.
2. ACL rule can be added, deleted, sorted.
   i. Rule can be added to a configured ACL. Regular ID number range is 1-500 .
   ii. Configured ACL can be deleted regularly. If the specified ACL instance number or rule number hasn't been configured, a false message will return.
   iii. Many rules of an ACL can be sorted and only need to specify the place where rule number need to be moved.
3. An ACL can become valid according to configured time range. After configuring absolute or relative time range on the switch, time range can be applied to the rule of ACL. This causes the rule to be valid according to the time range specification.
4. ZXR10 2920/2928/2952/2936-FI provides the following five types of ACLs:
   i. Basic ACL: Only match source IP address.
   ii. Extended ACL: Match source IP address, destination IP address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, ICMP type, ICMP Code and DiffServ Code Point (DSCP).
   iii. L2 ACL: Match source MAC address, destination MAC address, source VLAN ID and 802. 1p priority value.
   iv. Match Source IPV4/IPV6 address, destination IPV4/IPV6 address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, DiffServ Code Point (DSCP),

source MAC address, destination MAC address, source VLAN ID and 802. 1p priority value.

v. Global ACL: Match source IP address, destination IP address, IP protocol type, TCP source port number, TCP destination port number, UDP source port number, UDP destination port number, DiffServ Code Point (DSCP), source MAC address, destination MAC address, source VLAN ID and 802.1p priority value.

5. Each ACL has an access list number to identify. The access list number is a number. The access list number ranges of different types of ACL are shown below:
   - Basic ACL: 1~99
   - Extended ACL: 100~199
   - L2 ACL: 200~299
   - Hybrid ACL: 300~399, support IPV6
   - global ACL: 400

   Each ACL has at most 500 rules and the range is 1-500.

Basic Configuration of ACL

To configure ACL, perform the following steps.

1. To create a basic ACL instance, use the following command.

Command	Function
zte(cfg)#**config acl basic number** <*acl-number*>	This creates a basic ACL instance.

2. To create an extended ACL instance, use the following command.

Command	Function
zte(cfg)#**config acl extend number** <*acl-number*>	This creates an extended ACL instance.

3. To create a L2 ACL instance, use the following command.

Command	Function
zte(cfg)#**config acl link number** <*acl-number*>	This creates a L2 ACL instance.

4. To create a Hybrid ACL instance, use the following command.

Command	Function
zte(cfg)#**config acl hybrid number** <*acl-number*>	This creates a Hybrid ACL instance.

5. To create a global ACL instance, use the following command.

Command	Function
zte(cfg)#**config acl global**	This creates a global ACL instance. ACL number is 400.

6. To configure a basic ACL rule in basic ACL configuration mode, use the following command.

Command	Function
zte(cfg)#**rule** <*rule-id*>{**permit** | **deny**}{<*source-ipaddr wildcard*>| **any**}[**fragment**]	This configures a basic ACL rule in basic ACL configuration mode.

- < rule-id >: designate the sub-item of the access control list and the range is 1~500.
- source-ipaddr: The source IP or host of sending packet, expressed by 32 bits of IP address (in dotted decimal notation).
- source-wildcard: Wildcard, used as the source, expressed by 32 bits of IP address (in dotted decimal notation). The keyword any is used as the abbreviation for the source 0.0.0.0 and the wildcard 255.255.255.255.
- fragment: It is only available in fragment packet.

Creating a basic ACL instance means entering the configuration mode of this instance, that is , basic ACL configuration mode.

7. To configure an extended ACL rule, use the following command.

Command	Function
zte(cfg)#**rule** <*rule_id*>{**permit** | **deny**}{<*ip-protocol*>| **ip** | **tcp** | **udp** | **icmp** | **arp**}{<*source-ipaddr wildcard*>| **any**}{<*destination-ipaddr wildcard*>| **any**}[**dscp** <*0-63*>][**fragment**]	This configures an extended ACL rule.

- rule-id: designate the sub-item of the access control list and the range is 1~500.
- < ip-protocol >, ip, tcp, udp, icmp , arp: the matching protocol type. It can be one of the above keyword or an integer representing IP protocol number from 0 to 255.
- destination-ipaddr: the matching destination IP address.
- destination-wildcard: the wildcard shielding code matching with destination. the keyword any is used as the

abbreviation for the destination 0.0.0.0 and the wildcard 255.255.255.255.

- dscp: the parameter is optional. The packet can be classified by the DSCP value and the range is 0~63.
- fragment: it is only available in fragment packet.

Creating an extended ACL instance means entering the configuration mode of this instance, that is , extended ACL configuration mode.

8. To configure a L2 ACL rule, use the following command.

Command	Function
`zte(cfg)#`**rule** <*rule-id*>{**permit** | **deny**}{**arp** | **ip** | **other** | **any**}[**cos**<*0-7*>][<*source-vlanid*>]{<*source-mac wildcard*>| **any** |<*destination-mac wildcard*>| **any**}	This configures a L2 ACL rule.

- rule-id: designate the sub-item of the access control list and the range is 1~500.
- arp, ip, other, any: protocol type of the Ethernet frame, other represents any Ethernet protocol type except ip and arp, any represents any Ethernet type.
- cos: 802.1p priority, the range is 0~7.
- source-vlanid: the source VLAN of the packet.
- source-mac: the source MAC address of the packet, any represents any MAC address.
- source-mac wildcard: wildcard of source MAC address of packet.
- destination-mac: the destination MAC of the packet.
- destination-mac wildcard: the destination MAC address of the packet. Any represents any source MAC address.

Creating a L2 ACL instance means entering the configuration mode of this instance, that is , L2 ACL configuration mode.

9. To configure a Hybrid ACL rule, use the following command.

Command	Function
`zte(cfg)#`**rule** <*rule-id*>{**permit** | **deny**}{<*ip-protocol*>| **ip** | **tcp** | **udp** | **arp** | **any** || **all**}{<*source-ipaddr wildcard*>|**any**}{<*destination-ipaddr wildcard*>| **any**}[**dscp**<*0-63*>][**fragment**][**cos**<*0-7*>][<*source-vlanId*>][<*source-mac wildcard*>| **any**][<*destination-mac wildcard*>| **any**]	This configures a Hybrid ACL rule.

- rule-id: designate the sub-item of the access control list and the range is 1~500.
- ip-protocol, ip, tcp, udp, arp, any, all: the matching protocol. It can be one of the above keyword ip, tcp, udp and arp or an integer representing IP protocol number from 0

to 255. Any represents the protocol except ipv6. All represents all of the packets.

- dscp: the parameter is optional. The packet can be classified by the DSCP value and the range is 0~63.
- fragment: It is only available in fragment packet. The ip layer must be ipv4 address.

The ip layer must be ipv4 address. Creating a hybrid ACL instance means entering the configuration mode of this instance, that is , hybrid ACL configuration mode.

10. To configure an IPV6 ACL rule, use the following command.

Command	Function
zte(cfg)#**rule** <*rule-id*>{**permit** | **deny**}{<*ip-protocol*>| **tcp** | **udp** | **any**}{<*source-ipaddr wildcard*>| **any**}[<*source-port sourceport-mask*>]{<*destination-ipaddr wildcard*>| **any**}[<*dest-port destport-mask*>][<*vlanId*>]	This configures an IPv6 ACL rule.

- rule-id: Designate the sub-item of the access control list and the range is 1~500.
- ip-protocol, tcp, udp, any: the matching protocol. It can be one of the keyword "tcp"and "udp" or an integer representing IP protocol number from 0 to 255, any represents ignoring the protocol type.
- source-port: It is only available when configuring tcp and udp, the range is 0~65535 and the well-known port can be chosen.
- source-portmask: It is only available when configuring tcp and udp, can be the integer of 0~65535 or hex.
- dest-port: It is only be available when configuring tcp and udp, the range is 0~65535 and the well-known port can be chosen.
- dest-portmask: It is only be available when configuring tcp and udp, can be the integer of 0~65535 or hex.
- vlanId: The source VLAN of the packet. The ip layer here must be ipv6 address.

The ip layer here must be ipv6 address. Creating a IPV6 ACL instance means entering the configuration mode of this instance, that is , IPV6 ACL configuration mode.

11. To configure a global ACL rule, use the following command.

Command	Function
zte(cfg)#**rule** <*rule-id*>{**permit** | **deny**}{<*port-id*>| **any**}{<*ip-protocol*>| **ip** | **tcp** | **udp** | **arp** | **any**}{<*source-ipaddr wildcard*>| **any**}{<*destination-ipaddr wildcard*>| **any**}[**dscp** <*0-63*>][**fragment**][**cos** <*0-7*>][<*source-vlanId*>][<*source-mac wildcard*>| **any**][<*destination-mac wildcard*>| **any**]	This configures a global ACL rule.

- rule-id: designate the sub-item of the global access control list and the range is 1~16.
- ip-protocol, ip, tcp, udp, arp, any: the matching protocol. It can be one of the keyword "tcp", "udp", "arp"and "ip" or an integer from 0 to 255 representing IP protocol. any represents ignoring the protocol type.

Creating a global ACL instance means entering the configuration mode of this instance, that is , global ACL configuration mode.

12. To sort the rules in ACL instance, use the following command.

Command	Function
zte(cfg)#**move** <*rule-id*>{**after** | **before**}<*rule-id*>	This sorts the rules in ACL instance.

13. To delete a rule in ACL instance, use the following command.

Command	Function
zte(cfg)#**clear rule** <*rule-id*>	This deletes a rule in ACL instance.

14. To show the information of a configured ACL instance, use the following command.

Command	Function
zte(cfg)#**show acl config** [<*acl-number*>|<*acl-name*>][**rule** <*rule-id*>| **permit** | **deny** | **active** | **passive** | **snmp** | **command** | **policy** | **ports**]	This shows the information of a configured ACL instance.

15. To display ACL configuration information of port, use the following command.

Command	Function
zte(cfg)#**show acl binding** {**all** | **port** [<*portlist*>]| **trunk** [<*trunklist*>]}	This displays ACL configuration information of port.

16. To show the commands that can be used on ACL configuration mode, use the following command.

Command	Function
zte(hybrid-acl-group)#**list**	This displays the commands that can be used on ACL configuration mode.

This command is only used on ACL configuration mode, and then all the commands on this ACL mode will be shown.

17. To configure ACL information on port, use the following command.

Command	Function
zte(cfg)#**set port** <*portlist*> **acl** <*acl-number*>{**enable** | **disable**}	This sets ACL information on port.

18. To set ACL information on trunk port, use the following command.

Command	Function
zte(cfg)#**set trunk** <*trunklist*> **acl** <*acl-number*>{**enable** | **disable**}	This sets ACL information on trunk port.

19. To delete ACL instance, use the following command.

Command	Function
zte(cfg)#**clear acl** {**basic** | **extend** | **link** | **hybrid**} **number** <*acl-number*>	This deletes ACL instance.

20. To configure time-range, use the following command.

Command	Function
zte(cfg)#**set time-range** <*name*> **range** {**period** | **absolute**}<*start-time*> **to** <*end-time*>{**daily** | **day-off** | **day-working** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday**}	This configures time-range.

Day-off implies Saturday and Sunday. Day-working implies from Monday to Friday.

21. To bind ACL rule with the time-range, use the following command.

Command	Function
zte(cfg)#**set time-range** <*name*> **acl** <*acl-number*> **rule** <*rule-id*>{**enable** | **disable**}	This binds ACL rule with the time-range.

22. To clear the configuration of time-range, use the following command.

Command	Function
zte(cfg)#**clear time-range** <*name*>	This clears the configuration of time-range.

23. To display the configuration of time-range, use the following command.

Command	Function
zte(cfg)#**show time-range** [<*name*>]	This displays the configuration of time-range.

24. To configure the name of ACL instance, use the following command.

Command	Function
zte(cfg)#**set acl-name** <*acl-number*> **name** <*word*>	This sets ACL name.

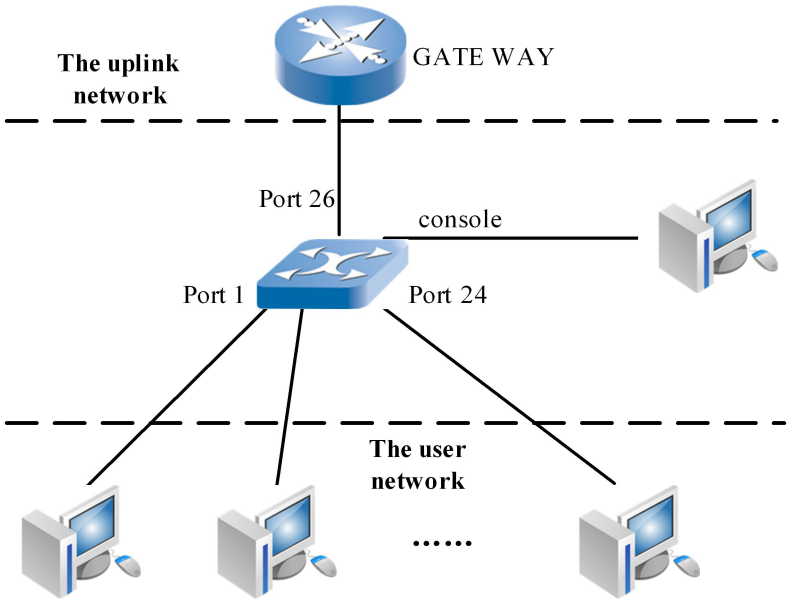
25. To clear the name of ACL instance, use the following command.

Command	Function
zte(cfg)#**clear acl-name** <*acl-number*>	This clears ACL name.

ACL Configuration Example

As shown in Figure 68, configure ACL in the switch to realize the following functions. Forbid the users to access the exterior net through the gateway from 9:00 to 18:00. The gateway connects with the switch on port 26. The client PC connects switch on port 1-24. All the users access the exterior network through the gateway 192.168.0.1.

FIGURE 68 ACL CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#config acl hybrid number 300
zte(hybrid-acl-group)#rule 1 deny ip any 192.168.0.1 255.255.255.255
zte(hybrid-acl-group)#exit
zte(cfg)#set port 1-24 acl 300 enable
zte(cfg)#set time-range worktime range period 09:00 to 18:00 daily
zte(cfg)#set time-range worktime acl 300 rule 1 enable
```

Configuration detection:

```
/*after finishing the configuration, view ACL binding
state that all the ports are binding with ACL300.*/
zte(cfg)#show acl binding all
  Id    PortType   AclNo
  ----    ---------- -  ------
  1      PhyPort     300
  2      PhyPort     300
  3      PhyPort     300
  4      PhyPort     300
  .        .          .
  .        .          .
  .        .          .
22     PhyPort     300
  23     PhyPort     300
  24     PhyPort     300
```

1. ACL is not available in the time-range of 18:00-24:00 and 0:00-9:00.

```
zte(cfg)#show time-range
/*show time-range configuration. The time range activity is passive*/
  Supported  time-range number: 32
  Configured time-range number: 1
  name               activity    type      range
  ----------------   ----------  --------  -----------   ---------------
  worktime           passive     period    09:00 to 18:00 daily
zte(cfg)#show acl config 300
/*show the detailed configuration of ACL 300. The ACL state
binding with time-range is passive.*/
  Acl No      : 300
  Acl Name    :
  Acl Type    : hybrid
  Rule Number : 1
  ------------------------------------------------------------------
  RuleId    : 1
```

```
  State     : passive
  Filter    : deny ip any 192.168.0.1 255.255.255.255
  TimeRange : worktime
```

2. ACL is available only in the time-range of 9:00-18:00.

```
zte(cfg)#show time-range
/*show time-range configuration. The time range activity is active*/
  Supported  time-range number: 32
  Configured time-range number: 1
  name               activity    type      range
  ----------------   ----------  --------  ------------------------------
  worktime           active     period    09:00 to 18:00 daily
zte(cfg)#show acl config 300
/*show the detailed configuration of ACL 300.
The ACL state binding with time-range is active. */
  Acl No      : 300
  Acl Name    :
  Acl Type    : hybrid
  Rule Number : 1
  ----------------------------------------------------------------
  RuleId    : 1
  State     : active
  Filter    : deny ip any 192.168.0.1 255.255.255.255
  TimeRange : worktime
```

QoS Configuraton

QoS Overview

The switch provides the QoS function and the priority control function. The priority of the data packets can be determined by the source MAC address priority of the data packets, VLAN priority, 802.1P user priority, layer 3 DSCP priority, or the default port priority. The priority of a data packet is determined in the following sequence:

1. Priority of the data packets sent by CPU (determined by CPU).
2. Priority of the MGMT data packets (management data packets such as the BPDU packets). The priority of the management packets is determined by the initialization.
3. Priority of the static source MAC address.
4. VLAN priority.
5. 802.1P user priority.
6. Layer 3 DSCP priority.
7. Default port priority.

After the data packet priority is determined by the previous priority determination policy, the later policies are ignored. To use the default port priority to decide the priority of the data packets received by the port, all the following conditions shall be satisfied.

- The data packets are not data packets sent by CPU or management data packets.
- The source MAC address of the data packets cannot be the static address or the port source priority function is disabled.

- Priority of the VLAN that the data packets belong to is disabled, or Priority of the VLAN of the port belongs to is disabled.
- The 802.1P user priority of the port is disabled, or the data packets are not TAG data packets.
- Port DSCP priority is disabled.

After the priority control policy of the switch is configured, if the switch receives the data frames, the data frames with higher priority can be transmitted first to ensure the key applications.

Basic Configuration of QoS

The configurations of QoS on ZXR10 2920/2928/2952/2936-FI include global-based QoS configuration and port-based QoS configuration. This topic mainly introduces how to configure global-based QoS. The port-based QoS configuration will be introduced on the part of port configuration.

1. To set the mapping between 802.1P user priority and the queue on 100M port, use the following command.

Command	Function
`zte(cfg)#`**set qos priority-map feport user-priority** *<0-7>* **traffic-class** *<0-3>*	This sets the mapping between 802.1P user priority and the queue on 100M port.

2. To set the mapping between 802.1P user priority and the queue on gigabit port, use the following command.

Command	Function
`zte(cfg)#`**set qos priority-map geport user-priority** *<0-7>* **traffic-class** *<0-7>*	This sets the mapping between 802.1P user priority and the queue on gigabit port.

3. To set the mapping between IP DSCP priority and queue priority on 100M port, use the following command.

Command	Function
`zte(cfg)#`**set qos priority-map feport ip-priority** *<0-63>* **traffic-class** *<0-3>*	This sets the mapping between IP DSCP priority and queue priority on 100M port.

4. To set the mapping between IP DSCP priority and queue priority on gigabit port, use the following command.

Command	Function
zte(cfg)#**set qos priority-map geport ip-priority** <*0-63*> **traffic-class** <*0-7*>	This sets the mapping between IP DSCP priority and queue priority on gigabit port

5. To set the mapping between IP DSCP priority and user priority on gigabit port, use the following command.

Command	Function
zte(cfg)#**set qos priority-map geport ip-priority** <*0-63*> **user-priority** <*0-7*>	This sets the mapping between IP DSCP priority and user priority on gigabit port.

6. To configure the weight of port queue on 100M port, use the following command.

Command	Function
zte(cfg)#**set qos queue-schedule feport queue0-weight** <*1-32*> **queu e1-weight** <*1-32*> **queue2-weight** <*1-32*> **queue3-weight** <*1-32*>	This configures the weight of port queue on 100M port.

There are 4 100M queues, queue0-weight <1-32> is the weight of queue 0, queue1-weight <1-32> is the weight of queue 1, queue2-weight <1-32> is the weight of queue 2, queue3-weight <1-32> is the weight of queue 3.

7. To configure the weight of queue-schedule on gigabit port, use the following command.

Command	Function
zte(cfg)#**set qos queue-schedule geport session** <*0,1*> **queue** <*0-7*>{**sp** | **sdwrr** <*0,1*> **weight** <*1-32*>}	This configures the weight of queue-schedule on gigabit port.

The gigabit port has 8 queues (0-7). sp is the absolute priority mode. sdwrr number has sdwrr0 and sdwrr1. Weight <1-32> is the queue weight number.

8. To configure the schedule mode of 100M port, use the following command.

Command	Function
zte(cfg)#**set queue-schedule feport** <*port-list*>{ **wrr0** | **wrr1-sp** | **wrr2-sp** | **sp**}	This configures the schedule mode of 100M port.

- wrr0: queue 3, 2, 1 and 0 all adopt WRR mode.

- wrr1-sp: queue 3 adopts SP mode, queues 2,1,0 adopt WRR mode.
- wrr2-sp: queues 3, 2 adopt SP mode, queues 1,0 adopt WRR mode.
- sp: queues 3, 2, 1, 0 adopt SP mode.
- sp: absolute priority mode.
- wrr: Weighted Round mode.

9. To configure the schedule mode of gigabit port, use the following command.

Command	Function
zte(cfg)#**set queue-schedule geport** <*port-list*> **session** <*0,1*>	This configures the schedule mode of gigabit port.

10. To configure traffic supervision mode, use the following command.

Command	Function
zte(cfg)#**set qos policer counter-mode** {**L1** | **L2** | **L3**}	This configures traffic supervision mode.

- L1: include preamble+IPG+CRC
- L2: include L2+L3+header+CRC
- L3: include L3+packet without CR

Set counter mode of the qos policer. By default, it works in L2 mode.

11. To configure the committed speed(kbps) of the traffic monitor, use the following command.

Command	Function
zte(cfg)#**set qos policer** <*policerid,0-255*> **parameters** <*32-25165824*>	This configures the committed speed(kbps) of the traffic monitor.

12. To enable or disable the counter function on traffic monitor, use the following command.

Command	Function
zte(cfg)#**set qos policer** < *policerid,0-255*> **counter** <*0-15*>{**enable** | **disable**}	This enables or disables the counter function on traffic monitor.

13. To configure the overspeed disposal of the traffic monitor, use the following command.

Command	Function
zte(cfg)#**set qos policer** <*policerid,0-255*> **exceed-action** {**no-operation** | **drop**}	This configures the overspeed disposal of the traffic monitor.

14. To set the global ARP rate-limit, use the following command.

Command	Function
zte(cfg)#**set qos rate-limit arp-All** {**enable** | **disable**}	This sets the global ARP rate-limit.

- enable: ARP rate-limit is valid for all arp packets.
- disable: ARP rate-limit is only valid for the broadcast packet.
- All the 100M ports are enabled by default.

15. To configure ingress rate limit on 100M port, use the following command.

Command	Function
zte(cfg)#**set bandwidth feport** <*portlist*> **ingress session** <*0-3*> **rate** <*64-100000*>	This configures ingress rate limit on 100M port.

The parameter **session** <*0-3*> is configured as follows by default.

- 0: broadcast suppression
- 1: multicast suppression
- 2: rate limit
- 3: user configure

16. To configure packet type of port ingress rate limit on 100M port, use the following command.

Command	Function
zte(cfg)#**set bandwidth feport** <*portlist*> **ingress session** <*0-3*> **packet-type** {**unknowmulticast** | **broadcast** | **unicast** | **multicast** | **MGMT** | **ARP** | **tcp-control** | **tcp-data** | **udp** | **non-tcpudp**}{**enable** | **disable**}	This configures packet type of port ingress rate limit on 100M port.

17. To configure queue type of port ingress rate limit on 100M port, use the following command.

Command	Function
zte(cfg)#**set bandwidth feport** <*portlist*> **ingress session** <*0-3*> **queue-priority** <*queuelist*>{**enable** | **disable**}	This configures queue type of port ingress rate limit on 100M port.

18. To configure if port ingress rate limit includes management packet, use the following command. (management packet refers to layer 2 protocol message such as BPDU 01 80 C2 00 00 00)

Command	Function
zte(cfg)#**set bandwidth feport** <*portlist*> **ingress session** <*0-3*> **mgmt-no-ratelimit** {**enable** | **disable**}	This configures if port ingress rate limit includes management packet (management packet refers to layer 2 protocol message such as BPDU 01 80 C2 00 00 00).

19. To configure if enable each session of port ingress rate limit on 100M port, use the following command.

Command	Function
zte(cfg)#**set bandwidth feport** <*portlist*> **ingress session** <*0-3*>{**enable** | **disable**}	This configures if enable each session of port ingress rate limit on 100M port.

20. To configure the egress rate limit on 100M port, use the following command.

Command	Function
zte(cfg)#**set bandwidth feport** <*portlist*> **egress** {{**on rate** <*64-100000*>}| **off**}	This configures the egress rate limit on 100M port.

21. To configure the ingress rate limit on gigabit port, use the following command.

Command	Function
zte(cfg)#**set bandwidth geport** <*portlist*> **ingress** {{**on rate** <*2000-100M/1G*>}| **off**}	This configures the ingress rate limit on gigabit port.

22. To configure the egress rate limit on gigabit port, use the following command.

Command	Function
zte(cfg)#**set bandwidth geport** *<portlist>* **egress** {**on rate** *<281-100M/1G>*[**burstsize** *<4-16380>*]}| **off**}	This configures the egress rate limit on gigabit port.

The parameter **burstsize** *<4-16380>*: the unit is kbyte.

23. To configure packet type of port ingress rate limit on gigabit port, use the following command.

Command	Function
zte(cfg)#**set bandwidth geport** *<portlist>* **packet-type** { **unicast** | **nounicast** | **multicast** | **broadcast** }{**enable** | **disable**}	This configures packet type of port ingress rate limit on gigabit port.

24. To remark the VLAN attribution of the designated flow, use the following command.

Command	Function
zte(cfg)#**set policy vlan-remark in acl** *<1-400>* **rule** *<1-500><1-4094>*{**nested** | **replaced**{**untagged**|**tagged**|**all**}}	This remarks the VLAN attribution of the designated flow.

rule *<1-500>*, if global ACL, only 16 rules is supported.

25. To limit and measure the data flow rate according to the flow, use the following command.

Command	Function
zte(cfg)#**set policy policing in acl** *<1-400>* **rule** *<1-500>* **policer** *<0-255>*	This limits and measures the data flow rate according to the flow.

26. To copy the specified data flow to the monitor port, use the following command.

Command	Function
zte(cfg)#**set policy mirror in acl** *<1-400>* **rule** *<1-500>*{**cpu**|**analyze-port**}	This copies the specified data flow to the monitor port.

27. To redirect the specified data flow to the user-specified egress port, use the following command.

Command	Function
zte(cfg)#**set policy redirect in acl** *<1-400>* **rule** *<1-500>*{**cpu**|**port** *<portid>*}	This redirects the specified data flow to the user-specified egress port.

28. To implement flow statistic for the data flow matching ACL rule, use the following command.

Command	Function
zte(cfg)#**set policy statistics in acl** <*1-400*> **rule** <*1-500*> **counter** <*0-31*>	This implements flow statistic for the data flow matching ACL rule.

29. To remark the flow, use the following command.

Command	Function
zte(cfg)#**set police remark in acl** <*1-400*> **rule** <*1-500*> **up** <*0-7*>	This remarks the flow.

30. To clear flow monitor counter, use the following command.

Command	Function
zte(cfg)#**clear policy-counter** <*0-31*>	This clears flow monitor counter.

31. To delete QoS mirror matching a flow, use the following command.

Command	Function
zte(cfg)#**clear policy mirror in acl** <*1-400*> **rule** <*1-500*>	This deletes QoS mirror matching a flow.

32. To clear VLAN remark matching a flow, use the following command.

Command	Function
zte(cfg)#**clear policy vlan-remark in acl** <*1-400*> **rule** <*1-500*>	This clears VLAN remark matching a flow.

33. To clear QoS policing matching a flow, use the following command.

Command	Function
zte(cfg)#**clear policy policing in acl** <*1-400*> **rule** <*1-500*>	This clears QoS policing matching a flow.

34. To clear flow-based remark, use the following command.

Command	Function
zte(cfg)#**clear policer remark in acl** *<1-400>* **rule** *<1-500>*	This clears flow-based remark.

35. To clear QoS statistics matching a flow, use the following command.

Command	Function
zte(cfg)#**clear policy statistics in acl** *<1-400>* **rule** *<5-100>*	This clears QoS statistics matching a flow.

36. To clear QoS redirection matching a flow, use the following command.

Command	Function
zte(cfg)#**clear policy redirect in acl** *<1-400>* **rule** *<1-500>*	This clears QoS redirection matching a flow.

37. To view the mapping that between 802.1P user priority and queue priority, use the following command.

Command	Function
zte(cfg)#**show qos priority-map user-priority**	This views the mapping that between 802.1P user priority and queue priority.

38. To view the mapping that between IP DSCP priority and queue priority, use the following command.

Command	Function
zte(cfg)#**show qos priority-map ip-priority**	This views the mapping that between IP DSCP priority and queue priority.

39. To view global queue schedule, use the following command.

Command	Function
zte(cfg)#**show qos queue-schedule** [**wrr0** | **sp** | **wrr1-sp** | **wrr2-sp**]	This views global queue schedule.

40. To show all the QoS policer or a specified policer, use the following command.

Command	Function
zte(cfg)#**show qos policer** [*<0-255>*]	This views all the QoS policers or a specified policer.

41. To view all the qos policy counters, use the following command.

Command	Function
zte(cfg)#**show qos counter** [*<0-31>*]	This views all the qos policy counters.

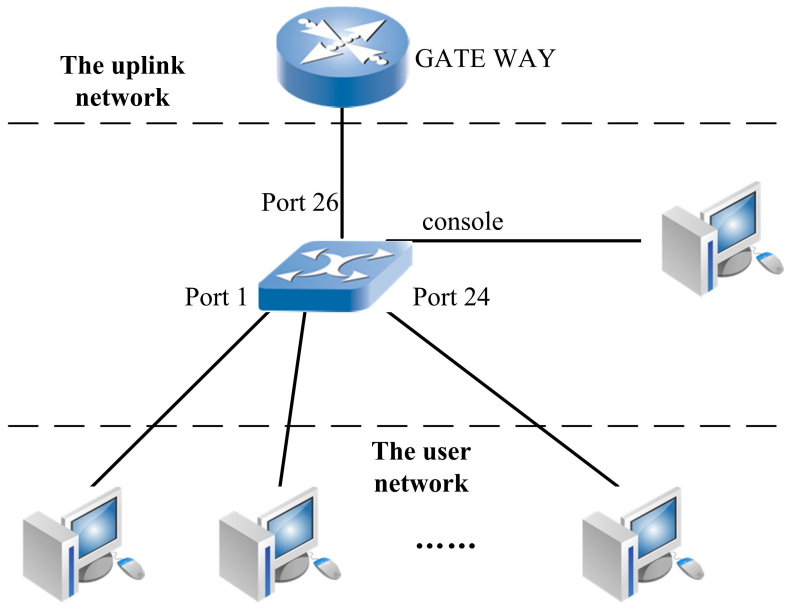
42. To view flow-based QoS application configuration, use the following command.

Command	Function
zte(cfg)#**show policy** [**qos-remark** | **mirror** | **redirect** | **vlan-remark** | **statistic** | **policing** [*<0-255>*]]	This views flow-based QoS application configuration.

QoS Configuration Example

As show in Figure 69, set the bandwidth (both direction) of all the user-interface as 2M. The uplink bandwidth of the switch is 20M. The uplink port is port 26 and the client PC accesses the network through port 24.

FIGURE 69 QOS CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#set bandwidth feport 1-24 ingress session 3 rate 2000
```

```
zte(cfg)#set bandwidth feport 1-24 ingress session 3 enable
zte(cfg)#set bandwidth feport 1-24 egress on rate 2000
zte(cfg)#set bandwidth geport 26 egress on rate 20000
zte(cfg)#show port 22 bandwidth session 3
/*view the ingress bandwidth configuration of ports 1-24 */
    PortId :  22
    IngressRateLimit session 3: enable
    Rate : 2000(kbps)
    Packet Type  :
      Unknown Multicast
      Broadcast
      Multicast
      Unicast
      MGMT
      ARP
      TCP-Data
      TCP-Ctrl
      UDP
      NON-TCPUDP
    MGMT-No-ratelimit: disable
    Queue-Priority 0: enable
    Queue-Priority 1: enable
    Queue-Priority 2: enable
    Queue-Priority 3: enable
zte(cfg)#show port 22 qos
/*view the Qos configuration of port 22*/
    PortId :  22
    PortQoSParams:
    UserPriority    : enable           DscpPriority   : disable
    DefaultPriority : 0                QueueSchedule(feport)  : WRR0
    PortPriorityRemapTable:
    COS(802.1p user priority),  RMP(Remapped priority)
    COS 0   1   2   3   4   5   6   7
    RMP 0   1   2   3   4   5   6   7
    IngressRateLimit session 0: disable
    IngressRateLimit session 1: disable
    IngressRateLimit session 2: disable
    IngressRateLimit session 3: enable
    EgressRateLimit :2000
zte(cfg)#show port 26 qos           /*view the Qos configuration of port 26*/
    PortId :  26
    PortQoSParams:
    UserPriority    : enable           DscpPriority   : disable
    DefaultPriority : 0         QueueSchedule(geport/sub card) :session 0
    PortPriorityRemapTable:
    COS(802.1p user priority),  RMP(Remapped priority)
    COS 0   1   2   3   4   5   6   7
    RMP 0   1   2   3   4   5   6   7
    ingress bandwidth information :
    ---------------------------------------
    current state : off
    packet type   : broadcast multicast unicast nounicast

    egress bandwidth information :
    ---------------------------------------
    current state : on
    config rate   : 20000(kbps)
    real rate     : 19951(kbps)
    burst size    : 4(kbyte)
```

Layer 2 Protocol Transparent Transmission Configuration

802.1x Transparent Transmission Overview

IEEE 802.1x is a Port-Based Network Access Control protocol. Port-based network access control is a way to authenticate and authorize the users to be connected to the LAN equipment. This type of authentication provides a point-to-pint subscriber identification method in the LAN.

ZXR10 2920/2928/2952/2936-FI provides 802.1x transparent transmission function which transparently transmits 802.1x protocol packets from the client to the authentication server for authentication.

ZXR10 2920/2928/2952/2936-FI provides 802.1x transparent transmission function. It also provides layer-2 transparent transmission function such as STP, LACP/OAM, ZGMP and GVRP. The protocol range is 0x00, 0x02-0x2f.

The common layer 2 protocols are shown below.

Protocol Number	Protocol
0x00	STP
0x02	LACP/OAM
0x03	802.1x
0x09	ZGMP
0x21	GVRP

Basic Configuration of Layer 2 Protocol Transparent Transmission

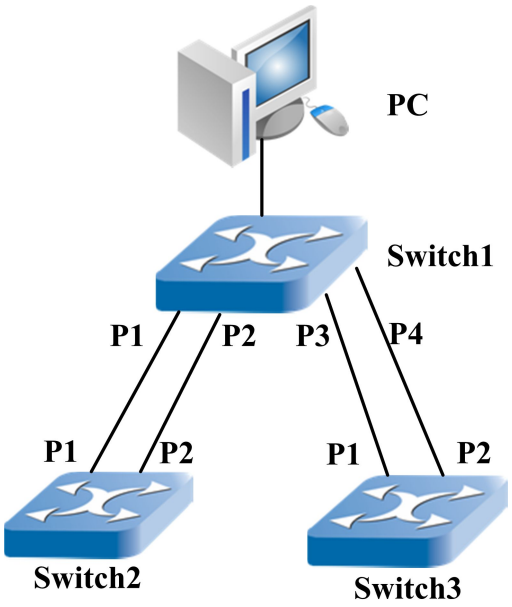
To configure layer 2 Protocol transparent transmission, perform the following steps.

Command	Function
zte(cfg)#**set l2pt** <*protocol-list*>{**enable** | **disable** | **invalid**}	This enables or disables L2pt transparent transmission function. enable is to enable layer 2 transparent transmission, disable is to disable layer 2 transparent transmission, invalid is to make layer 2 transparent invalid. All the layer 2 transparent protocols are invalid by default.
zte(cfg)#**show l2pt**	This displays the configuration of L2pt transparent transmission.

Layer 2 Protocol Transparent Transmission Configuration Example

As shown in Figure 70, set the LACP transparent transmission function of L2pt of switch1 to implement the link aggregation between switch2 and switch3. The configuration increases the link bandwidth and realizes the redundant backup.

FIGURE 70 L2PT CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#set lacp enable
zte(cfg)#set lacp aggregator 1 add port 1, 2
```

```
zte(cfg)#set l2pt 0x02 enable
zte(cfg)#set vlan 100 enable
zte(cfg)#set vlan 100 add port 1, 3
zte(cfg)#set vlan 200 enable
zte(cfg)#set vlan 200 add port 2, 4
zte(cfg)#sho lacp aggregator 1
/*show the aggregation state of switch2 and switch3 in the system view*/
  Group 1
     Actor                          Partner
  ------------------------ ------------------------------
  Priority    :32768                        32768
  Mac      :00.d0.d0.02.00.54              00.d0.d0.29.52.06
  Key      :258                          258
  Ports      :2, 1                          2, 1
```

Layer 3 Configuration

Layer 3 Overview

ZXR10 2920/2928/2952/2936-FI provides a few layer 3 functions for the remote configuration and management. To realize the remote access, an IP port must be configured on the switch. If the IP port of the remote configuration host and that of the switch are not in the same network segment, it is also necessary to configure the static route.

Static route is a simple unicast route protocol. The next-hop address to a destination network segment is specified by user, where next hop is also called gateway. Static route involves destination address, destination address mask, next-hop address, and egress interface. Destination address and destination address mask describe the destination network information. The next-hop address and egress interface describe the way that switch forwards destination packet.

ZXR10 2920/2928/2952/2936-FI allows adding and deleting the static ARP table. ARP table records mapping relationship between IP address and MAC address of each node in same network. When sending IP packets, switch first checks whether destination IP address is in the same network segment. If yes, switch checks whether there is a peer end IP address and MAC address mapping entry in ARP table.

1. If yes, switch directly sends the IP packets to this MAC address.
2. If MAC address corresponding to peer end IP address cannot be found in ARP table, an ARP Request broadcast packet will be sent to the network to query peer end MAC address.

Generally, entries of the ARP table on the switch are dynamic. Static ARP table entry need to be configured only when the connected host cannot respond the ARP Request.

To configure the layer 3 function, use command **config router** to enter into layer 3 configuration mode first.

Basic Configuration of Layer 3

To configure L3 function, perform the following steps.

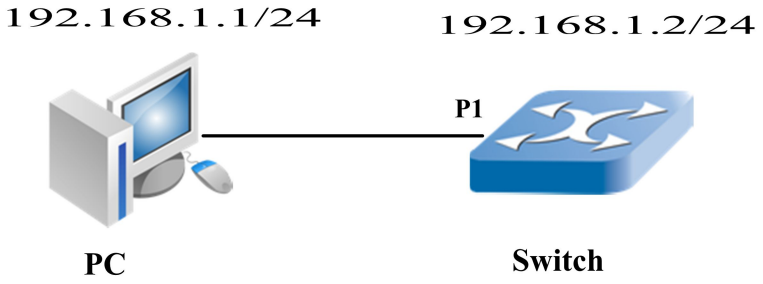
Command	Function
zte(cfg)#**arp add** *<A.B.C.D><HH.HH.HH.HH.HH.HH><0-63><1-4094>*	This adds static ARP.
zte(cfg)#**arp delete** *<A.B.C.D>*	This deletes static ARP.
zte(cfg)#**arp ipport** *<0-63>* **timeout** *<1-1000>*	This sets the timeout of layer-3 port. The parameter **timeout**: the default is 10, the unit is minute.
zte(cfg)#**clear arp**	This deletes all the arp information.
zte(cfg)#**clear ipport** *<0-63>*[**mac**|**ipaddress** {*<A.B.C.D/M>*|*<A.B.C.D><A.B.C.D>*}|**vlan** *<vlanname>*]	This deletes ipport configuration.
zte(cfg)#**clear iproute** [{*<A.B.C.D/M>*|*<A.B.C.D><A.B.C.D>*}*<A.B.C.D>*]	This deletes static route.
zte(cfg)#**iproute** {*<A.B.C.D/M>*|*<A.B.C.D><A.B.C.D>*}*<A.B.C.D>*[*<1-15>*]	This adds static route.
zte(cfg)#**set ipport** *<0-63>*{**enable**|**disable**}	This enables or disables layer-3 port.
zte(cfg)#**set ipport** *<0-63>* **ipaddress** {*<A.B.C.D/M>*|*<A.B.C.D><A.B.C.D>*}	This sets IP address and submask of layer-3 port.
zte(cfg)#**set ipport** *<0-63>* **mac** *<HH.HH.HH.HH.HH.HH>*	This sets the MAC address of layer-3 port
zte(cfg)#**set ipport** *<0-63>* **vlan** *<vlanname>*	This sets the VLAN binding with layer 3 port.
zte(cfg)#**show arp** [**static** | **dynamic** | **invalid** | **ipport** *<0-63>*[**static** | **dynamic** | **invalid**]| **ipaddress** *<A.B.C.D>*]	This shows arp information.
zte(cfg)#**show ipport** [*<0-63>*]	This shows layer-3 port information.
zte(cfg)#**show iproute**	This shows all the static routes.

Layer 3 Configuration Example

As shown in Figure 71, configure layer-3 ip address as 192.168.1.2 on switch. The ip address 192.168.1.2 can ping through PC ad-

dress 192.168.1.1. Bind vlan100 with 192.168.1.2. Port 1 on switch connects with PC.

FIGURE 71 LAYER-3 CONFIGURATION EXAMPLE



Configuration of switch:

```
zte(cfg)#set vlan 100 en
zte(cfg)#set vlan 100 add port 1 untag
zte(cfg)#set port 1 pvid 100
zte(cfg)#config route
zte(cfg-router)#set ipport 0 ipaddress 192.168.1.2 255.255.255.0
zte(cfg-router)#set ipport 0 vlan 100
zte(cfg-router)#set ipport 0 enable
zte(cfg-router)#show ipport
IpPort  En/Disable  IpAddress  Mask  MacAddress  VlanId
------ -------- ------------- ------ --------    --------
  0     enabled  192.168.1.2  255.255.255.0  00.d0.d0.fa.29.20     100
zte(cfg-router)#ex
zte(cfg)#ping 192.168.1.1
/*use the command ping to see whether the layer-3 port is available.*/
zte(cfg)#ping 192.168.1.1
  Reply from 192.168.1.1 : bytes=28 time<1ms TTL=64
  Reply from 192.168.1.1 : bytes=28 time<1ms TTL=64
  Reply from 192.168.1.1 : bytes=28 time<1ms TTL=64
  Reply from 192.168.1.1 : bytes=28 time<1ms TTL=64
  Reply from 192.168.1.1 : bytes=28 time<1ms TTL=64
```

Access Service Configuration

Access Service Overview

With the rapid expansion of Ethernet construction scale, to meet the fast increase of subscribers and requirement of diversified broadband services, Network Access Service (NAS) is embedded on the switch to improve the authentication and management of access subscribers and better support the billing, security, operation, and management of the broadband network.

NAS uses the 802.1x protocol and RADIUS protocol to realize the authentication and management of access subscribers. It is highly efficient, safe, and easy to operate.

IEEE 802.1x is called port-based network access control protocol. Its protocol system includes three key parts: client system, authentication system, and authentication server.

1. The client system is generally a user terminal system installed with the client software. A subscriber originates the IEEE802.1x protocol authentication process through this client software. To support the port-based network access control, the client system must support the Extensible Authentication Protocol Over LAN (EAPOL).
2. The authentication system is generally network equipment that supports the IEEE802.1x protocol, for example, the switch. Corresponding to the ports of different subscribers (the ports could be physical ports or MAC address, VLAN, or IP address of the user equipment), the authentication system has two logical ports: controlled port and uncontrolled port.
   - The uncontrolled port is always in the state that the bidirectional connections are available. It is used to transfer the EAPOL frames and can ensure that the client can always send or receive the authentication.
   - The control port is enabled only when the authentication is passed. It is used to transfer the network resource and services. The controlled port can be configured as bidirectional controlled or input controlled to meet the requirement of different applications. If the subscriber authentication is not passed, this subscriber cannot visit the services provided by the authentication system.

     The controlled port and uncontrolled port in the IEEE 802.1x protocol are logical ports. There are no such physical ports on the equipment. The IEEE 802.1x protocol sets up a local authentication for each subscriber that other subscribers cannot use. Thus, there will not be such a problem that the port is used by other subscribers after the port is enabled.
3. The authentication server is generally a RADIUS server. This server can store a lot of subscriber information, such as VLAN that the subscriber belongs to, CAR parameters, priority, subscriber access control list, and so on. After the authentication of a subscriber is passed, the authentication server will pass the information of this subscriber to the authentication system, which will create a dynamic access control list. The subsequent flow of the subscriber will be monitored by the above parameters. The authentication system communicates with the RADIUS server through the RADIUS protocol.

RADIUS is a protocol standard used for the authentication, authorization, and exchange of configuration data between the Radius server and Radius client.

RADIUS adopts the Client/Server mode. The Client runs on the NAS. It is responsible for sending the subscriber information to the specified Radius server and carrying out operations according to the result returned by the server.

The Radius Authentication Server is responsible for receiving the subscriber connection request, verifying the subscriber identity, and returning the configuration information required by the customer. A Radius Authentication Server can serve as a RADIUS customer proxy to connect to another Radius Authentication Server.

The Radius Accounting Server is responsible for receiving the subscriber billing start request and subscriber billing stop request, and completing the billing function.

The NAS communicates with the Radius Server through RADIUS packets. Attributes in the RADIUS packets are used to transfer the detailed authentication, authorization, and billing information. The attributes used by this switch are primarily standard attributes defined in the rfc2865, rfc2866, and rfc2869.

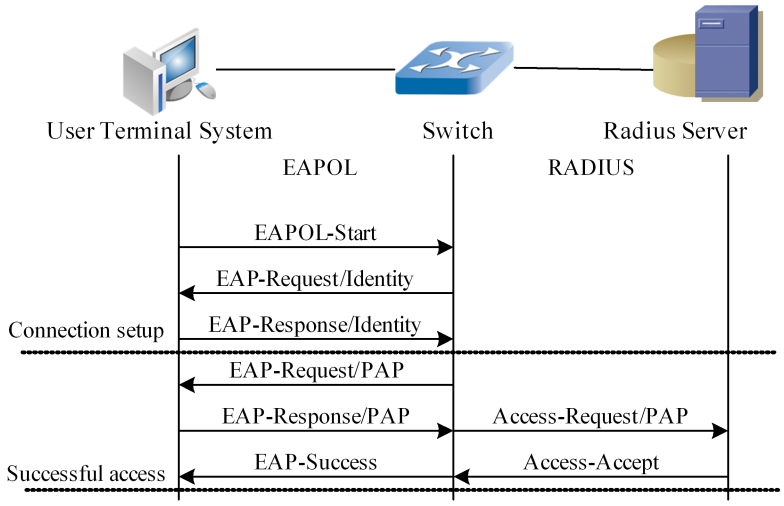
The EAP protocol is used between the switch and the subscriber. Three types of identity authentication methods are provided between the RADIUS servers: PAP, CHAP, and EAP-MD5. Any of the methods can be used according to different service operation requirements.

- PAP (Password Authentication Protocol)

  PAP is a simple plain text authentication mode. NAS requires the subscriber to provide the username and password and the subscriber returns the subscriber information in the form of plain text. The server checks whether this subscriber is available and whether the password is correct according to the subscriber configuration and returns different responses. This authentication mode features poor security and the username and password transferred may be easily stolen.

  Figure 72 shows the process of using the PAP mode for identity authentication.

FIGURE 72 USING PAP MODE FOR IDENTITY AUTHENTICATION



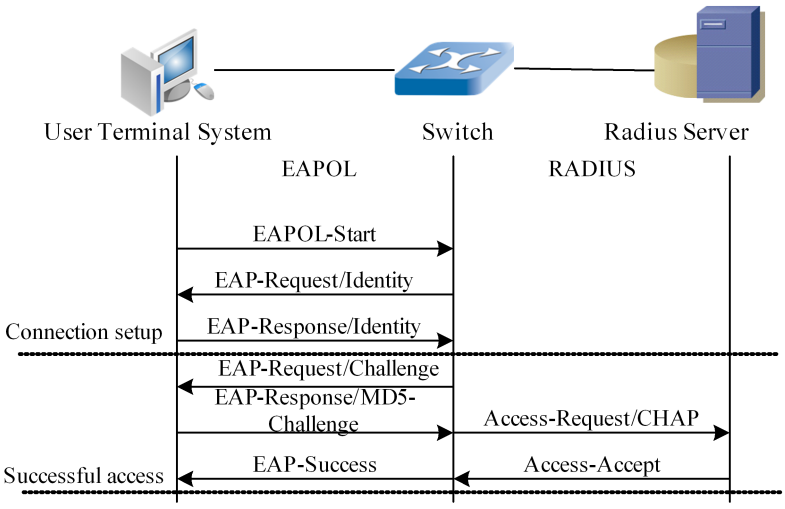
- CHAP (Challenge Handshake Authentication Protocol)

  CHAP is an encrypted authentication mode and avoids the transmission of the user's real password upon the setup of connection. NAS sends a randomly generated Challenge string to the user. The user encrypts the Challenge string by using the own password and MD5 algorithm and returns the username and encrypted Challenge string (encrypted password).

The server uses the user password it stores and the MD5 algorithm to encrypt the Challenge string. Then it compares this Challenge string with the encrypted password of the server and returns a response accordingly.

Figure 73 shows the process of using the CHAP mode for identity authentication.

FIGURE 73 USING CHAP MODE FOR IDENTITY AUTHENTICATION

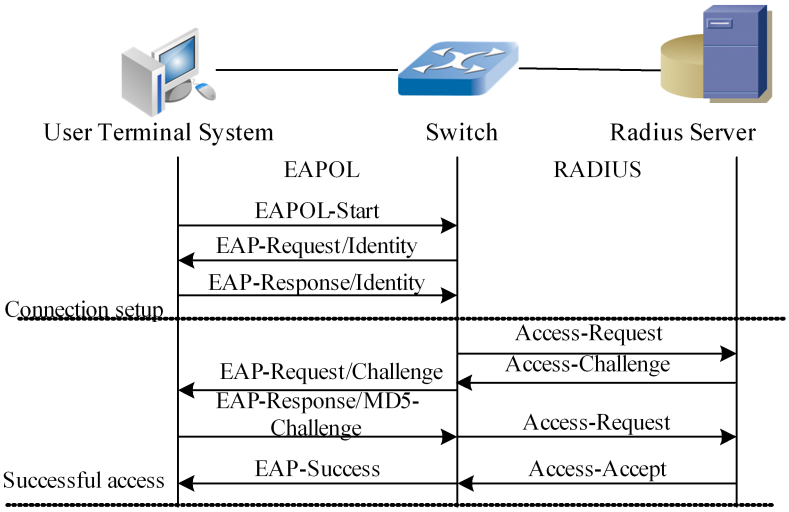


- EAP (Extensible Authentication Protocol)

  EAP is a kind of authentication mode of transmitting EAP message transparently including EAP-MD5 and PEAP. The following example is about EAP-MD5 description.

  EAP-MD5 is a CHAP identity authentication mechanism used in the EAP framework structure. Figure 74 shows the process of using the EAP-MD5 mode for identity authentication.

FIGURE 74 USING EAP MODE FOR IDENTITY AUTHENTICATION



Basic Configuration of Access Service

Command	Function
`zte(cfg-nas)#`**aaa-control port** <*portlist*> **dot1x** {**enable**|**disable**}	This enables/disables the port 802.1x function.
`zte(cfg-nas)#`**aaa-control port** <*portlist*> **accounting** {**enable**|**disable**}	This enables/disables port accounting function.
`zte(cfg-nas)#`**aaa-control port** <*portlist*> **max-hosts** <*0-256*>	This sets the maximum number of subscribers connected through the port. 0 indicates non-limit.
`zte(cfg-nas)#`**aaa-control port** <*portlist*> **multiple-hosts** {**enable**|**disable**}	This allows/prohibits multi-subscriber access of the port.

Command	Function
zte(cfg-nas)#**aaa-control port** <*portlist*> **port-mode** {**auto**|**force-unauthorized**|**force-authorized**}	This configures the authentication control mode of the port. **auto**: enable 802.1X authentication on port. **force-unauthorized**: The authorization will be forced to deny no matter it is valid or invalid. **force-authorized**: the authorization will be forced to pass no matter it is valid or invalid.
zte(cfg-nas)#**aaa-control port** <*portlist*> **protocol** {**pap**|**chap**|**eap**}	This sets the authentication mode of the port.
zte(cfg-nas)#**aaa-control port** <*portlist*> **keepalive** {**enable**|**disable**}	This enables/disables the abnormal off-line detection mechanism of the port. When the function is enabled, vlanjump and private MAC address are not supported to be used at the same time.
zte(cfg-nas)#**aaa-control port** <*portlist*> **keepalive period** <*1-3600*>	This sets the abnormal off-line detection period of the port. The unit is second, the default is 10s.
zte(cfg-nas)#**dot1x max-request** <*1-10*>	This sets the maximum times of request resending when the timer expires before the authentication system receives the Challenge response from the client. The default is 2.
zte(cfg-nas)#**dot1x quiet-period** <*0-65535*>	This sets the interval between the first authentication failure of the authentication system and the next authentication request. The unit is second, the default is 60s.
zte(cfg-nas)#**dot1x re-authenticate** {**enable**|**disable**}	This enables/disables re-authentication mechanism.

zte(cfg-nas)#**dot1x re-authenticate period** <*1-4294967295*>	This sets the re-authentication period. The unit is second, the default is 3600s.
zte(cfg-nas)#**dot1x server-timeout** <*1-65535*>	This sets the timeout time for the authentication system to receive the data packets from the authentication server. The unit is second, the default is 30s.
zte(cfg-nas)#**dot1x supplicant-timeout** <*1-65535*>	This sets the timeout time for the authentication system to receive the data packets from the authentication client system. The unit is second, the default is 30s.
zte(cfg-nas)#**dot1x tx-period** <*1-65535*>	This sets the time that the authentication system needs to wait before it can resend the EAPOL data packet because it does not receive the response from the client. The unit is second, the default is 30s.
zte(cfg-nas)#**dot1x add vlan** <*vlanid*>[**mac** <*HH.HH.HH.HH.HH.HH*>]	This configures the private MAC address that DOT1X protocol can use.
zte(cfg-nas)#**dot1x delete vlan** <*vlanid*>	This deletes the private MAC address that DOT1X protocol can use.
zte(cfg-nas)#**radius isp** <*ispname*>{**enable**|**disable**}	This adds/deletes an ISP domain. The length of ISP name can not be more than 32 characters.
zte(cfg-nas)#**radius isp** <*ispname*> **add accounting** <*A.B.C.D*>[<*0-65535*>]	This adds an accounting server to the domain.
zte(cfg-nas)#**radius isp** <*ispname*> **delete accounting** <*A.B.C.D*>	This deletes an accounting server from the domain.
zte(cfg-nas)#**radius isp** <*ispname*> **add authentication** <*A.B.C.D*>[<*0-65535*>]	This adds an accounting server to the domain.

zte(cfg-nas)#**radius isp** <*ispname*> **delete authentication** <*A.B.C.D*>	This deletes the authentication server from the domain.
zte(cfg-nas)#**radius isp** <*ispname*> **defaultisp** {**enable**|**disable**}	This specifies a default domain.
zte(cfg-nas)#**radius isp** <*ispname*> **description** <*string*>	This configures the domain description.
zte(cfg-nas)#**radius nasname** <*nasname*>	This sets the NAS server name.
zte(cfg-nas)#**radius isp** <*ispname*> **client** <*A.B.C.D*>	This sets the IP address of the client in the domain.
zte(cfg-nas)#**radius isp** <*ispname*> **fullaccount** {**enable**|**disable**}	This sets/deletes the full account of the domain.
zte(cfg-nas)#**radius isp** <*ispname*> **sharedsecret** <*string*>	This configures the shared password of a domain.
zte(cfg-nas)#**radius retransmit** <*1-255*>	This sets the number of retransmissions upon server response timeout. The default is 3.
zte(cfg-nas)#**radius timeout** <*1-255*>	This sets the server response timeout time.
zte(cfg-nas)#**radius keep-time** <*0-4294967295*>	This configures keep time of radius accounting breaking packet. **keep-time**<*0-4294967295*> unit is second, default value is 0 which means non restriction.
zte(cfg-nas)#**radius delimiter** <*ispdelimiter*>	This configures Radius authentication domain name delimiter. The domain name delimiter is @ by default.
zte(cfg-nas)#**clear accounting-stop** {**session-id** <*session-id*>|**user-name** <*user-name*>|**isp-name** <*isp-name*>|**server-ip** <*A.B.C.D*>}	This deletes the radius accounting-stop packet which is failed to send.

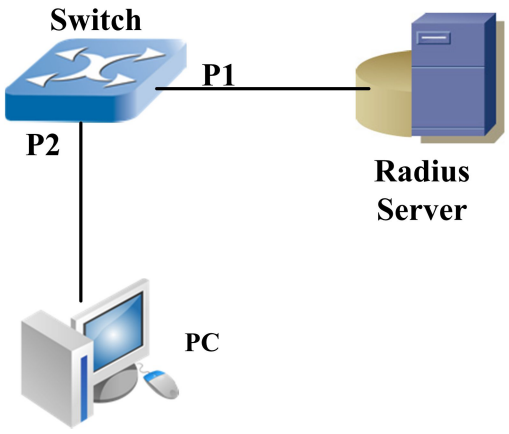
zte(cfg-nas)#**show radius accounting-stop** [{**session-id** <*session-id*>| **user-name** <*user-name*>| **isp-name** <*isp-name*>| **server-ip** <*A.B.C.D*>}]	This shows radius configuration.
zte(cfg)#**show aaa-control port** [<*portlist*>]	This shows the 802.1x configuration of port .
zte(cfg)#**show dot1x**	This shows 802.1x protocol parameters.
zte(cfg)#**show client**	This shows the information of all accessing users.
zte(cfg)#**show client index** <*0-255*>	This shows the information of an accessing users.
zte(cfg)#**show client mac** <*HH.HH.HH.HH.HH.HH*>	This shows the user accessing information of a MAC address.
zte(cfg)#**show client port** <*portlist*>	This shows the user accessing information of a port.

zte(cfg)#**show radius** [**ispname** <*ispname*>]	This shows radius configuration information.
zte(cfg-nas)#**clear client**	This deletes all clients.
zte(cfg-nas)#**clear client index** <*0-255*>	This clears one client.
zte(cfg-nas)#**clear client port** <*portlist*>	This clears client of one port.
zte(cfg-nas)#**clear client vlan** <*vlantlist*>	This clears all clients on one VLAN.

Access Service Configuration Example

As shown in Figure 75, the user installs radius client terminal in PC. The switch connects the radius server and the user's PC through the network cable. The user can log in to the switch through the console port and configure the access server, and then enable client software on user PC to originate authentication request.

FIGURE 75 ACCESS AUTHENTICATION CONFIGURATION EXAMPLE



1. configure dot1x commands

```
zte(cfg)#set port 2 security enable
zte(cfg)#config nas
zte(cfg-nas)#aaa port 2 dot1x enable
zte(cfg-nas)#aaa port 2 keepalive enable
zte(cfg-nas)#aaa port 2 accounting enable
```

2. configure radius commands

```
zte(zte)#config nas
zte(cfg-nas)#radius isp zte enable
zte(cfg-nas)#radius isp zte defaultisp enable
zte(cfg-nas)#radius isp zte sharedsecret isam
zte(cfg-nas)#radius isp zte client 192.168.20.20
zte(cfg-nas)#radius isp zte add accounting 192.168.20.199 1812
zte(cfg-nas)#radius isp zte add authentication 192.168.20.199 1813
```

3. Enable radius client software on PC and input correct username and password. Then the authentication request is launched. When the authentication request succeeds, view the user information by using the command show client.

```
zte(cfg)#show client
  MaxClients   : 256      HistoryAccessClientsTotal : 1
  OnlineClients: 1        HistoryFailureClientsTotal: 0

Index UserName Authorized PortId VlanId  MacAddress ElapsedTime
----- -------- ---------- ------ ------  ------------
------------
0   zhouzhou     yes       2      1    00.0a.eb.93.10.23 0:0:0:7
```

Caution:

Disable the security proxy such as Sygate before the user PC sending authentication request.

Syslog Configuration

Syslog Overview

Syslog is an important part of Ethernet switch and is the information junction center of system software module. Syslog manages most of important information output and classifies in detail , which filters the information effectively and provides the strong support for network administrator and development staff to monitor network running status and diagnose network fault.

Syslog is classified by information source and information is filtered by function module, which satisfies user customized demand.

As shown in Table 14, syslog can classify the log information from the top down into eight levels according to importance. Information filters from low level to high level.

TABLE 14 SYSLOG LOG INFORMATION

Severity Level	Description
Emergencies	crucial fault
Alerts	the fault that must be corrected quickly
Critical	key fault
Errors	the fault need to be noticed but not important
Warnings	warn , maybe a mistake exists
Notifications	the information that needs to be noticed
Informational	general prompt information
Debugging	debug information

Basic Configuration of Syslog

To configure Syslog, perform the following steps.

Command	Function
`zte(cfg)#`**set syslog** {**enable** | **disable**}	This enables or disables syslog. By default syslog is disabled.
`zte(cfg)#`**set syslog module** {**all**|**alarm**|**commandlog**|**radius**|**AAA**}{**enable**|**disable**}	This enables or disables syslog module.

Command	Function
zte(cfg)#**set syslog level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **informational** | **debugging**}	This defines syslog information level. The default level of syslog information is informational.
zte(cfg)#**set syslog add server** <*id,1-5*> **ipaddress** <*A.B.C.D*>[**name** <*string*>]	This sets syslog server. The server name can not be more than 20 characters.
zte(cfg)#**set syslog delete server** <*id*>	This deletes syslog server according to id.
zte(cfg)#**show syslog status**	This displays configuration of syslog.

Syslog Configuration Example

Suppose that syslog function of switch is enabled , information level is informational, all function modules are enabled, server IP address is 192.168.1.1, name is Srv1.

Configuration of switch:

```
zte(cfg)#set syslog level informational
zte(cfg)#set syslog add server 1 ipaddress 192.168.1.1 name Srv1
zte(cfg)#set syslog module all enable
zte(cfg)#set syslog enable
zte(cfg)#show syslog status
  Syslog status: enable
  Syslog alarm level: informational
 Syslog enabled modules:
  radius          alarm         AAA           commandlog
  Syslog server      IP          Name
  1           192.168.1.1       Srv1
```

NTP Configuration

NTP Overview

NTP is the protocol used to synchronize the clocks between network devices. ZXR10 2920/2928/2952/2936-FI provides NTP client function and synchronizes the clock with other NTP servers.

Basic Configuration of NTP

To configure NTP, perform the following steps.

Command	Function
zte(cfg)#**set ntp** {**enable** | **disable**}	This enables or disables NTP.
zte(cfg)#**set ntp authenticate** {**enable** | **disable**}	This enables or disable NTP authentication.
zte(cfg)#**set ntp add authentication-key** <*keyid*> **md5** <*string*>	This sets NTP authentication-key. < string > has 1–16 characters.
zte(cfg)#**set ntp add trusted-key** <*keyid*>	This sets NTP trusted-key.
zte(cfg)#**set ntp delete authentication-key** <*keyid*>	This deletes NTP authentication-key.
zte(cfg)#**set ntp delete trusted-key** <*keyid*>	This deletes NTP trusted-key.
zte(cfg)#**set ntp server** <*A.B.C.D*> **key** <*keyid*>	This sets NTP server key.
zte(cfg)#**set ntp clock-period** <*5-2147483647*>	This sets the period of NTP synchronization. The unit is second, the default is 10s.
zte(cfg)#**set ntp server** <*A.B.C.D*>[**version** <*1,2,3*>]	This sets ip address and version id of NTP server.
zte(cfg)#**set ntp source** <*A.B.C.D*>	This sets the source IP address that is used for switch to send NTP packet.
zte(cfg)#**set ntp timezone** <*(-12)-(+13)*>	This sets NTP time-zone.
zte(cfg)#**show ntp**	This views the current status and configuration information of NTP module.

NTP Configuration Example

Suppose that switch and NTP server (IP address is 202.10.10.10) implement time synchronization. Make sure that switch and NTP server can ping each other successfully. The NTP module is configured as follows:

```
zte(cfg)#set ntp server 202.10.10.10
zte(cfg)#set ntp enable
zte(cfg)#show ntp
  ntp protocol is enable
  ntp protocol version : 3
  ntp server address   : 202.10.10.10
  ntp source address   : None
  ntp is_synchronized  : No
  ntp rcv stratum      : 16
```

```
  no reference clock.
ntp time zone        : 0
```

In the viewed information, ntp is-synchronized means if the current switch is synchronized with server.

OAM

OAM Overview

OAM Overview

With the rapid development of Ethernet technology, Ethernet networking proportion gradually increases in network structure . Ethernet devices replacing ATM network devices and other devices are widely used in access, convergence layer and backbone network. Due to the great application, Operation Administration Maintenance (OAM) function of Ethernet devices receive much concern. The main Ethernet OAM protocols are shown below.

- IEEE 802.3ah (Operations, Administration, and Maintenance-OAM)
- IEEE 802.1ag (Connectivity Fault Management) (Draft)
- ITU-Y 1731 (OAM functions and mechanisms for Ethernet based networks) (Draft)

OAM Function

OAM Protocol Function

IEEE 802.3ah operations, administration and maintenance standard is the formal standard, which aims at the management of link level. It monitors and troubleshoots the point to point (virtual point to point) Ethernet link. It has the important meaning for connection management of Last One Mile. The faults take place constantly on Last One Mile.

ZXR10 2900 series switch supports IEEE 802.3ah.

Ethernet OAM Main Function

Ethernet OAM function on ZXR10 2900 series switch can be classified into the following types.

1. OAM Discovery Function

   After enabling Ethernet OAM function, ZXR10 2900 series switch can detect the remote DTE device which has OAM function. After coordinating with the peer OAM, enter normal Ethernet OAM interaction process .

2. Remote Link Event Alarm

   OAM function inspects the events of remote link, and adopts the corresponding responding methods. When the fault takes place on remote link, OAM defines the event and announces

it to remote OAM client. The detailed events announcement packet is also provided.

OAM defines the following link events.

- Link Failure: The physical layer locates the failure that take place on receiving direction of local DTE.
- Emergency Failure: The local failure event has happened, and this failure can not be recovered.
- Emergency Events: The un-defined emergency event happens.

3. OAM Remote Loopback

   ZXR10 2900 series switch provides optional data link layer frame level loopback mode by OAM function. OAM remote loopback is used to locate failure and examine the link performance. When remote DTE is on the OAM remote loopback mode, the statistic data of local and remote DTE can be inquired and compared at any time. Meanwhile, OAM loopback frame can be analyzed to obtain the additional information of link health (frame discard due to the link failure).

4. Link Monitoring

   ZXR10 2900 series switch monitors and examines the link state, and announces the specified frame events by OAM function. The specified frame events can be classified into four types: error symbol period event, error frame event and error frame period event, error frame-second statistic event. After inspecting the error, OAM will respond and alarm the peer device by announcement mechanism.

Basic Configuration of OAM

To configure OAM, perform the following steps.

1. To enable or disable global OAM function, use the following command.

Command	Function
`zte(cfg)#` **set ethernet-oam** {**enable** | **disable**}	This enables or disables global OAM function.

2. To enable or disable OAM function on port, use the following command.

Command	Function
`zte(cfg)#` **set ethernet-oam port** <*portlist*>{**enable** | **disable**}	This enables or disables OAM function on port.

3. To configure OAM discovery period, timeout range and mode on port, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam port** <*portlist*> **period** <*1-10*> **timeout** <*2-20*> **mode** {**active** | **passive**}	This configures OAM discovery period, timeout range and mode on port.

The parameter **period** <*1-10*>: discovery period, 1 represents 10ms. 2 represents 20ms and so on. By default, 10 represents 100ms.

The parameter **timeout** <*2-20*>: timeout, by default it is 5 seconds

The parameter **mode** [**active** | **passive**]: discovery mode, it is active by default.

4. To start or stop OAM remote-loopback function on port, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam remote-loopback port** <*portlist*>{**start** | **stop**}	This starts or stops OAM remote-loopback function on port.

The prerequisites of enabling this function is that the global OAM function has been enabled, the OAM function has been enabled on destination port, and the OAM discovery process has been completed.

5. To set remote-loopback timeout value on port, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam remote-loopback timeout** <*1-10*>	This sets remote-loopback timeout value on port.

The parameter **timeout**: the default is 3s.

6. To enable or disable link monitor function, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam port** <*portlist*> **link-monitor** {**enable** | **disable**}	This enables or disables link monitor function.

7. To configure the symbol period event which is used for link monitor, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam port** <*portlist*> **link-monitor symbol-period threshold** <*1-65535*> **window** <*1-65535*>	This configures the symbol period event which is used for link monitor.

The symbol period is decided by the symbol number which is received during a specified period by switch, that is, a period is to collect a specified number of symbols. When the error symbol number is larger than the period receiving threshold, the link alarm will be appeared.

The parameter **threshold** <*1-65535*>: the error symbol collected in a period. It is 1 by default.

The parameter **window** <*1-65535*>: the symbol number period. The unit is million. For example, 30 represents that collecting 30,000,000 symbols is a period. It is 1 by default.

8. To configure the error frame, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam port** <*portlist*> **link-monitor frame threshold** <*1-65535*> **window** <*1-60*>	This configures the error frame.

The parameter **threshold** <*1-65535*>: the number of error frame. The default value is 1.

The parameter **window** <*1-60*>: time period. The default value is 1 second.

9. To configure the period of error frame, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam port** <*portlist*> **link-monitor frame-period threshold** <*1-65535*> **window** <*1-600000*>	This configures the period of error frame.

The frame period is decided by the frame number which is received during a specified period by switch, that is, a period is to collect a specified number of frames. When the error frame number is larger than the period receiving threshold, the link alarm will be appeared.

The parameter **threshold** <*1-65535*>: the error frame number, the default is 1.

The parameter **window** <*1-600000*>: the frame number, the default value is 100. the unit is thousand. 1 represents 1000.

10. To configure error frame summary, use the following command.

Command	Function
zte(cfg)#**set ethernet-oam port** <*portlist*> **link-monitor frame-seconds threshold** <*1-900*> **window** <*10-900*>	This configures error frame summary.

Error frame accumulation event is the accumulation seconds of error frame in a period which is generated by switch. When the error frame accumulation seconds is no less than the threshold, the error frame summary event will be generated.

The parameter **threshold** <*1-900*>: the accumulation seconds of error frame. The default value is 1 second.

The parameter **window** <*10-900*>: period,the default value is 60 seconds.

11. To show OAM configuration information, use the following command.

Command	Function
zte(cfg)#**show ethernet-oam** [**port** [<*portlist*>{ **discovery** | **statistics** | **link-monitor**}]]	This shows OAM configuration information.

When the command is used without any parameter, OAM global configuration information will be shown.

The parameter **port**: shows the port configuration information that OAM is enabled.

The parameter **discovery**: shows the OAM state and configuration information on local and the peer that is discovered by a specified port, including port OAM discovery period, mode, and the detection for relative link and the loopback.

The parameter **statistics**: shows the statistics information of link events on the designated ports.

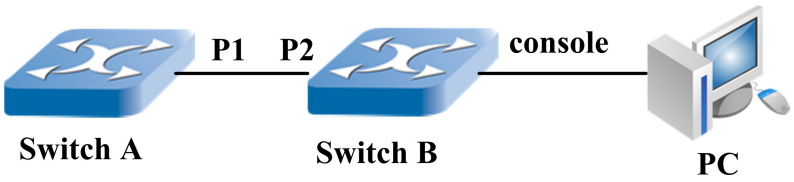
The parameter **link-monitor**: shows the link detection configuration information and the various error frames of the designated ports.

OAM Configuration Example

OAM Remote Loopback Configuration Example

OAM monitor function can notify the abnormal frame of link receiver to the local. The function is based on OAM discovery. The user logs in to the switch through console port and configures OAM. Enable OAM and the port link monitor of the other end. Then the error frame and the error symbol can be detected and notify local switch. A network structure is shown in Figure 76.

FIGURE 76 REMOTE LOOP NETWORK



Configuration of switch A:

```
zte(cfg)#set ethernet-oam en
zte(cfg)#set ethernet-oam port 1 en
```

Configuration of switch B:

```
zte(cfg)#set ethernet-oam enable
zte(cfg)#set ethernet-oam port 2 enable
zte(cfg)#show Ethernet-oam port 2 discovery
  PortId 2: ethernet oam enabled
  Local DTE               /*the local device information*/
    -----------
  Config:
    Mode   : active /*the port mode must be active, or the discovery is failure*/
    Period : 10*100(ms)
    Link TimeOut : 5(s)
    Unidirection : nonsupport
    PDU max size : 1518
  Status:
    Parser       : forward
    Multiplexer  : forward
    Stable       : yes
/*yes represents that discovery succeeds. no represents discovery fails.*/
    Discovery    : done
/*discovery succeeds. “undone” represents that discovery fails*/
    Loopback     : off
    PDU Revision : 92

  Remote DTE        /*the remote device information*/
    -----------
  Config:
    Mode   : active
    Link Monitor    : support
    Unidirection    : nonsupport
    Remote Loopback : support
Mib Retrieval   : nonsupport
    PDU max size    : 1518
  Status:
    Parser       : forward
    Multiplexer  : forward
Stable       : yes
Mac Address  : 00.d0.d0.29.28.02
/*the system MAC of the remote device.
The MAC address is 00.00.00.00.00.00 when discovery fails.*/
    PDU Revision : 967
zte(cfg)#set ethernet-oam remote-loopback port 2 start
zte(cfg)#show ethernet-oam port 2 discovery
  PortId 2: ethernet oam enabled
  Local DTE
  -----------
  Config:
    Mode   : active
    Period : 10*100(ms)
    Link TimeOut : 5(s)
    Unidirection : nonsupport
    PDU max size : 1518
  Status:
    Parser       : discard /*the parser state is discard*/
    Multiplexer  : forward
    Stable       : yes
    Discovery    : done
    Loopback     : on(Master)
/*the local is the active originator (Master). The other end displays as slave.*/
```

```
    PDU Revision : 1431

  Remote DTE
    -----------
  Config:
    Mode   : active
    Link Monitor    : support
    Unidirection    : nonsupport
    Remote Loopback : support
    Mib Retrieval   : nonsupport
    PDU max size    : 1518
  Status:
    Parser       : loopback     /*the parser state is loopback*/
    Multiplexer  : discard       /*the multiplexer state is discard*/
    Stable       : yes
    Mac Address  : 00.d0.d0.29.28.02
    PDU Revision : 28
zte(cfg)#set ethernet-oam remote-loopback port 2 stop
/*disable OAM remote-loopback on port2.
 The switch replies OAM discovery success.*/
```

The key points of configuration:

The switch gives the following prompts when OAM discovery failure occurs, or starting and stopping remote loopback.

OAM discovery is completed successfully on port 2, the following information appears.

```
SAT JUL 03 23:30:00 2004 ETH-OAM port 2's discovery process is successful.
```

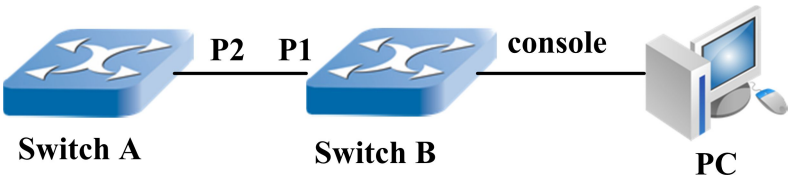
Disconnect the network cable between switches, the following information appears.

```
SAT JUL 03 23:33:00 2004 ETH-OAM port 2 deteced
 a fault in the local receive direction.
```

OAM Link Control Event Configuration Example

OAM monitor function can notify the abnormal frame of the link receiver to the local. The function is based on OAM discovery. The user logs in to the switch through console port and configures OAM. Enable OAM and the port link monitor of the other end. Then the error frame and the error symbol can be detected and announced to local switch.

FIGURE 77 LINK CONTROL NETWORK



Configuration of switch A:

```
zte(cfg)#set ethernet-oam enable
zte(cfg)#set ethernet-oam port 2 enable
```

Configuration of switch B:

```
zte(cfg)#set ethernet-oam enable
zte(cfg)#set ethernet-oam port 1 enable
zte(cfg)#set ethernet-oam port 1 link-monitor enable
zte(cfg)#set ethernet-oam port 1 lin symbol-period threshold 10 window 10
zte(cfg)#set ethernet-oam port 1 lin frame threshold 10 window 20
zte(cfg)#set ethernet-oam port 1 link-monitor frame-period threshold
```

```
5 window 1000
zte(cfg)#set ethernet-oam port 1 link-monitor frame-seconds threshold
10 window 30
zte(cfg)#show eth port 1 link-monitor
  Link Monitoring of Port: 1
  Errored Symbol Period Event:
    Symbol Window : 10(million symbols)
    Errored Symbol Threshold : 10
    Total Errored Symbols    : 0
    Local Total Errored Events  : 0
    Remote Total Errored Events : 0

  Errored Frame Event:
    Period Window : 20(s)
    Errored Frame Threshold : 10
    Total Errored Frames    : 0
    Local Total Errored Events  : 0
    Remote Total Errored Events : 0

  Errored Frame Period Event:
    Frame Window : 1000(ten thousand frames)
    Errored Frame Threshold : 5
    Total Errored Frames    : 0
    Local Total Errored Events  : 0
    Remote Total Errored Events : 0

  Errored Frame Seconds Event:
    Errored Seconds Window    : 30(s)
    Errored Seconds Threshold : 10(s)
    Total Errored Frame Seconds : 0(s)
    Local Total Errored Frame Seconds Events  : 0
Remote Total Errored Frame Seconds Events : 0
```

Key of configuration:

The link monitoring events are classified into four types: error symbol monitor event, error frame monitor event, error frame-period monitor event and error frame-second statistic monitor event. When the link monitoring information is viewed, the related error symbol, the statistic of error frame and the statistic of local and peer link events will be shown on each event.

Chapter 8

Network Management

Table of Contents

Remote-Access 193
SSH 195
SNMP 198
RMON 202
Cluster Management 205
SFLOW 213
WEB 214

Remote-Access

Remote-Access Overview

Remote-Access is a restrictive mechanism used for network management users to log in through TelnetSSHSNMPWeb, that is, it is used to restrict the access. This function is to enhance the security of the network management system.

After this function is enabled, specify a network management user to access the switch only from a specified IP address , the user cannot access the switch from other IP addresses. When this function is disabled, the network management user can access the switch through TelnetSSHSNMPWeb from any IP address.

Basic Configuration of Remote-Access

The Remote-Access configuration on the switch includes the following contents:

Command	Function
zte(cfg)#**set remote-access** {**any**|**specific**}	This disables/enables the restrictive access. The parameter any represents any IP address can access switch . The parameter specific represents only the permitted IP address can access switch.
zte(cfg)#**set remote-access ipaddress** <*A.B.C.D*>[<*A.B.C.D*>]{**snmp**|**telnet**|**ssh**|**web**}{**permit**|**deny**}	This permits/denies the login mode of IP address.
zte(cfg)#**set remote-access ipaddress**<*A.B.C.D*><*netmask*>[**snmp** | **telnet** | **ssh** | **web**]{**permit** | **deny**}	This configures the IP address, subnet mask and login mode of the switch which can be login. **[snmp** | **telnet** | **ssh** | **web**]{**permit** | **deny**} is used to configure the address-based hierarchical authorization, which restricts the login mode of remote login in detail. By default , all login modes are permitted.
zte(cfg)#**clear remote-access all**	This deletes all IP addresses of restrictive access.
zte(cfg)#**clear remote-access ipaddress** <*A.B.C.D*>[<*A.B.C.D*>]	This deletes an IP address of restrictive access.
zte(cfg)#**show remote-access**	This displays the remote-access configuration information.

Remote-Access Configuration Example

Example 1: Only allow the network management user to access the switch from 10.40.92.0/24 through Telnet SSH SNMP Web.

```
zte(cfg)#set remote-access specific
zte(cfg)#set remote-access ipaddress 10.40.92.0 255.255.255.0
zte(cfg)#show remote-access
  Whether check remote manage address: YES
  Allowable remote manage address(es) and application(s):
10.40.92.0/255.255.255.0 snmp, telnet, ssh, web
```

Example 2: Only allow the network management user to access the switch from 10.40.92.212 through Telnet SSH SNMP Web.

```
zte(cfg)#set remote-access specific
zte(cfg)#set remote-access ipaddress 10.40.92.212
zte(cfg)#show remote-access
  Whether check remote manage address: YES
  Allowable remote manage address(es) and application(s)::
    10.40.92.212/255.255.255.255 snmp, telnet, ssh, web
```

Example 3: Allow the network management user to access the switch from any IP address through Telnet SSH SNMP Web.

```
zte(cfg)#set remote-access any
zte(cfg)#show remote-access
  Whether check remote manage address: NO
```

Allowable remote manage address(es) and application(s):

any

SSH

SSH Overview

The secure shell (SSH) is a protocol created by Network Working Group of the IETF, which is used to offer secure remote access and other secure network services over an insecure network.

The purpose of the SSH protocol is to solve the security problems in interconnected networks, and to offer a securer substitute for Telnet and Rlogin (Although the present development of the SSH protocol has far exceeded the remote access function scope), therefore, the SSH connection protocol shall support interactive session.

The SSH can be used to encrypt all transmitted data. Even if these data is intercepted, no useful information can be obtained.

At present, the SSH protocol has two incompatible versions: SSH v1.x and SSH v2.x. This switch only supports SSH v2.0 and uses the password authentication mode. The SSH uses port 22.

Basic Configuration of SSH

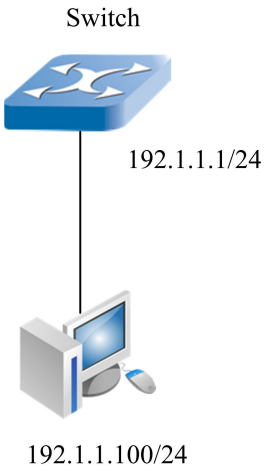
The SSH configuration on the switch includes the following contents:

Command	Function
`zte(cfg)#`**set ssh** {**enable**|**disable**}	This enables or disables SSH.
`zte(cfg)#`**show ssh**	This displays the SSH configuration and status.

SSH Configuration Example

As shown in Figure 78, one host attempts to access the switch through SSH. The switch is configured with a layer 3 port. The IP address of the port is 192.1.1.1/24, and the IP address of the host is 192.1.1.100/24.

FIGURE 78 SSH CONFIGURATION EXAMPLE



The specific configuration of the switch is as follows:

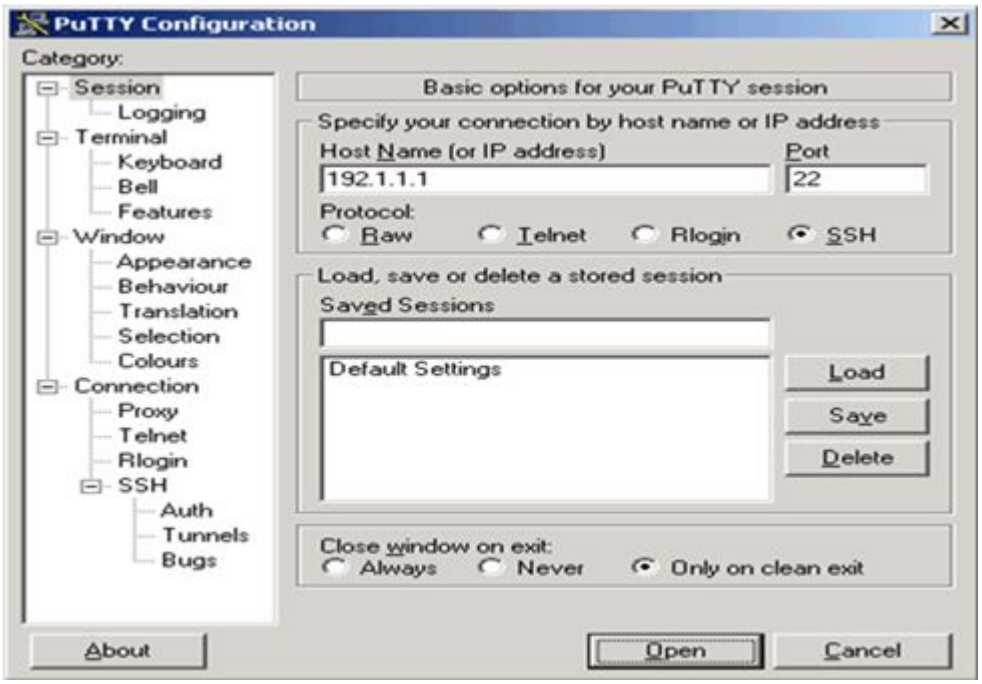
```
zte(cfg)#creat user zte
zte(cfg)#set login-password zte
zte(cfg)#set ssh enable
```

The client end setting of host:

The client end of SSH v2.0 can use the free software Putty developed by Simon Tatham . The current version provides client end support of Putty0.54 version. The required settings when using Putty to log in to switch are as follows.

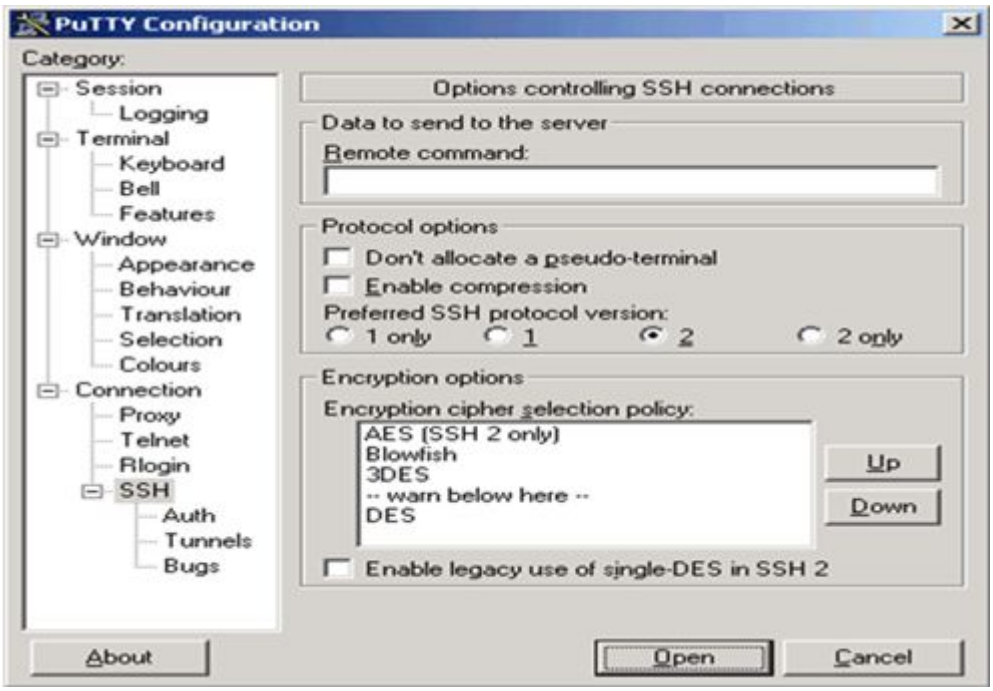
1. Set the IP address and port number of the SSH Server, as shown in Figure 79.

FIGURE 79 SETTING IP ADDRESS AND PORT NUMBER OF THE SSH SERVER



2. Set the SSH version number, as shown in Figure 80.

FIGURE 80 SETTING SSH VERSION NUMBER



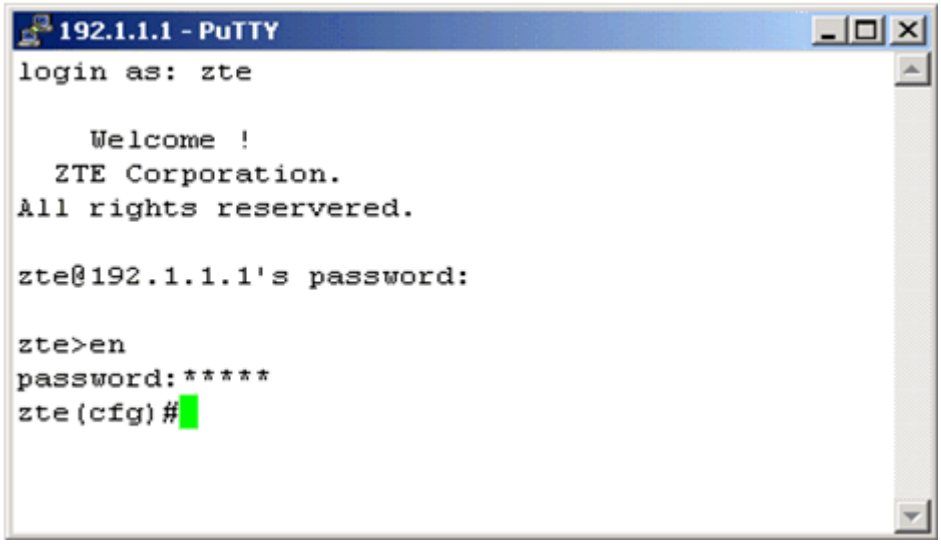
3. For the first time to log in, the user confirmation is needed, as shown in Figure 81.

FIGURE 81 USER CONFIRMATION REQUIRED IN THE FIRST LOGIN

PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's dss key fingerprint is:
ssh-dss 1024 9b:ad:bc:18:7e:9c:dd:4d:43:a8:16:d5:2b:9c:54:7a
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
是(Y)
否(N)
取消

4. The SSH login result is shown in Figure 82.

FIGURE 82 SSH LOGIN RESULT



SNMP

SNMP Overview

SNMP is the most popular network management protocol currently. It involves a series of protocol and specifications:

- MIB: Management Information Base
- SMI: Structure of Management Information
- SNMP: Simple Network Management Protocol

They offer the means to collect network management information from network devices. SNMP also enables devices to report problems and errors to network management stations. Any network administrator can use SNMP to manage switches. ZXR10 2900 supports SNMPv1 v2c and v3(v3 strengthens SNMP management security based on v1 and v2c).

SNMP adopts the "Management process—Agent process" model to monitor and control all types of managed network devices. The SNMP network management needs three key elements:

1. Managed devices, which can communicate over the Internet. Each device contains an agent.
2. NMS The network management process shall be able to communicate over the Internet.
3. The protocol used for the exchange of management information between the switching agent process and the NMS, that is, SNMP.

An NMS collects data by polling the agents that reside in the managed devices. The agents in the managed devices can report errors to NMSs at any time before the NMSs poll them. These errors are called traps. When a trap occurs to a device, the NMS can be used to query the device (suppose it is reachable) and obtain more information. Snmp v2c and v3 also support inform (a SNMPv2 Trap that need response) to inform abnormal events to NMS. If receives inform message NMS will send a acknowledgement packet to switch. If switch hasn't received acknowledgement packet from NMS in a period time it will resend the original inform message twice.

All variables in the network are stored in the MIB. SNMP monitors network device status by querying the related object values in the agent MIB. ZXR10 2900 implements the standard MIB and private MIB defined in rfc2233, rfc1493, rfc2665 and rfc2819.

Basic Configuration of SNMP

The SNMP configuration includes the following contents:

Command	Function
`zte(cfg)#` **config snmp**	This enters SNMP management mode.
`zte(cfg-snmp)#` **create community** <*string*>{**public** | **private**}	This creates communication name and set the access authority.
`zte(cfg-snmp)#` **create view** <*string*>[{**include** | **exclude**}<*mib-oid*>]	This creates a view name. The default setting is include, which includes mib subtree.

Command	Function
zte(cfg-snmp)#**set community** <*string*> **view** <*string*>	This sets specific community name that the view contains.
zte(cfg-snmp)#**set engineID** <*string*>	This sets engine ID.
zte(cfg-snmp)#**set group** <*string*> **v3** {**auth** | **noauth** | **priv**}[**read** <*string*>[**write** <*string*>[**notify** <*string*>]]]	This sets group name and security level.
zte(cfg-snmp)#**set host** <*A.B.C.D*>{**trap** | **inform**}{**v1** | **v2c**}<*string*>	This sets IP address, group name , username and version of trap host and inform host. Host is destination host that trap or inform sends. At the same time, specify trap or inform version and community or user.
zte(cfg-snmp)#**set host** <*A.B.C.D*>{**trap** | **inform**} **v3** <*string*>{**auth** | **noauth** | **priv**}	
zte(cfg-snmp)#**set trap** {**linkdown** | **linkup** | **authenticationfail** | **coldstart** | **warmstart** | **topologychange** | **memberupdown** | **portloopdetect** | **trunkloopdetect** | **dynamicMacExceed**|**remoteDiscovery**|**all**}{**enable** | **disable**}	This enables or disables SNMP link connection and disconnection, link authentication failure, cold boot, warm start, cluster topology change, cluster member up/down and loopdetect and so on.
zte(cfg-snmp)#**set user** <*username*><*groupname*> **v3** [{**md5-auth** | **sha-auth**}<*password*>][**des56-priv** <*password*>]	This sets SNMP v3 user name, group name, and its related authentication mode, password.
zte(cfg)#**show snmp** [**community** | **engineID** | **group** | **host** | **trap** | **user** | **view**]	This views SNMP information.
zte(cfg-snmp)#**clear community** <*string*>	This deletes community name.
zte(cfg-snmp)#**clear group** <*string*> **v3** {**auth** | **noauth** | **priv**}	This deletes group name.
zte(cfg-snmp)#**clear host** <*A.B.C.D*>{**trap** | **inform**}<*string*>	This deletes trap or inform host.
zte(cfg-snmp)#**clear user** <*string*> **v3**	This deletes username.
zte(cfg-snmp)#**clear view** <*string*>	This deletes viewname.

SNMP Configuration Example

Example 1 Suppose that the IP address of the network management server is 10.40.92.105, the switch has a layer 3 port with the IP address

of 10.40.92.200, and the switch is managed through the network management server.

Create a community named "zte" with the read/write authority and the view named "vvv", and then associate the community "zte" with the view "vvv". Specify the IP address of the host receiving traps as 10.40.92.105, and the community as "zte".

Configuration of switch:

```
zte(cfg)#config router
zte(cfg-router)#set ipport 0 ipaddress 10.40.92.200 255.255.255.0
zte(cfg-router)#set ipport 0 vlan 2
zte(cfg-router)#set ipport 0 enable
zte(cfg-router)#exit

zte(cfg)#config snmp
zte(cfg-snmp)#create community zte private
zte(cfg-snmp)#create view vvv
zte(cfg-snmp)#set community zte view vvv
zte(cfg-snmp)#set host 10.40.92.105 trap v1 zte

zte(cfg-snmp)#show snmp community
  CommunityName  Level      ViewName
  -------------- --------- ------------
  zte              private    vvv

zte(cfg-snmp)#show snmp view
  ViewName     Exc/Inc  MibFamily
  ----------- -------- ------------------------
  vvv           Include  1.3.6.1

zte(cfg-snmp)#show snmp host
  HostIpAddress     Comm/User   Version  type   SecurityLevel
  ---------------- ----------- ------- ------ -------------
  10.40.92.77        zte           Ver.1    Trap
```

Example 2 Suppose that the IP address of the network management server is 10.40.92.77, the switch has a layer 3 port with the IP address of 10.40.92.11, and the switch is managed through the network management server.

Create a user named "zteuser" and the group named "ztegroup", the security level of this group is private (that is authentication and encryption). Specify the IP address of the host receiving trap or inform as 10.40.92.77, and the user is"zteuser".

Configuration of switch:

```
zte(cfg)#config router
zte(cfg-router)#set ipport 1 ipaddress 10.40.92.11/24
zte(cfg-router)#set ipport 1 vlan 1
zte(cfg-router)#set ipport 1 enable
zte(cfg-router)#exit

zte(cfg)#config snmp
zte(cfg-snmp)# set group ztegroup v3 private
zte(cfg-snmp)# set user zteuser ztegroup v3 md5-auth zte des56-priv zte
zte(cfg-snmp)# set host 10.40.89.77 inform v3 zteuser priv

zte(cfg-snmp)#show snmp group
  groupName: ztegroup
  secModel : v3                        readView  : zteView
  secLevel : AuthAndPriv              writeView : zteView
  rowStatus: Active                    notifyView: zteView

zte(cfg-snmp)#show snmp user
  UserName   : zteuser
  GroupName  : ztegroup(v3)
  EngineID   : 830900020300010289d64401
  AuthType   : Md5                      StorageType: NonVolatile
  EncryptType: Des_Cbc                  RowStatus  : Active
```

```
zte(cfg-snmp)#show snmp host
  HostIpAddress     Comm/User   Version type    SecurityLevel
  ---------------- ----------- ------- ------ -------------
  10.40.89.77       zteuser      Ver.3   Inform  AuthAndPriv
```

RMON

RMON Overview

The Remote Monitoring (RMON) defines standard network monitoring function and the communication interface between the management console and the remote monitor. RMON offers an efficient and high availability method to monitor the behaviors of subnets in case of reducing the load of other agents and management stations.

RMON specifications refer to the definition of RMON MIB. ZXR10 2900 supports four groups of RMON MIB.

- History: records the periodic statistics sample of the information that can be obtained from the statistics group.
- Statistics: maintains the basic application and error statistics of each subnet that the agent monitors.
- Event: it is a table related to all events generated by RMON agents.
- Alarm: allows operators of the management console to set sampling interval and alarm threshold for any count or integer recorded by RMON agents.

All these groups are used to store the data collected by the monitor and the derived data and statistics. The alarm group is based on the implementation of the event group. These data can be obtained through the MIB browser.

The RMON control information can be configured through the MIB browser, and a HyperTerminal or remote Telnet command line. The RMON sampling information and statistics are obtained through the MIB browser.

Basic Configuration of RMON

To configure RMON, perform the following steps.

Command	Function
zte(cfg-snmp)#**set rmon** {**enable**|**disable**}	This enables or disables RMON function.
zte(cfg-snmp)#**set alarm** *<1-65535>*{**interval** *<1-65535>*| **variable** *<mib-oid>*| **sampletype** {**absolute** | **delta**}| **startup** {**rising** | **falling** | **both**}| **threshold** *<1-65535>* **eventindex** *<1-65535>*{**rising** | **falling**}| **owner** *<name>*| **status** {**valid** | **underCreation** | **createRequest** | **invalid**}}	This sets alarm group.
zte(cfg-snmp)#**set event** *<1-65535>*{**description** *<string>*| **type** {**none** | **log** | **snmptrap** | **logandtrap**}| **owner** *<name>*| **community** *<name>*| **status** {**valid** | **underCreation** | **createRequest** | **invalid**}}	This sets event group.
zte(cfg-snmp)#**set history** *<1-65535>*{**datasource** *<portname>*| **bucketRequested** *<1-65535>*| **owner** *<name>*| **interval** *<1-3600>*| **status** {**valid** | **underCreation** | **createRequest** | **invalid**}}	This sets history group.
zte(cfg-snmp)#**set statistics** *<1-65535>*{**datasource** *<portname>*| **owner** *<name>*| **status** {**valid** | **underCreation** | **createRequest** | **invalid**}}	This sets statistics group.
zte(cfg-snmp)#**show alarm** [*<1-65535>*]	This displays configuration information about alarm group.
zte(cfg-snmp)#**show event** [*<1-65535>*]	This displays configuration information about event group.
zte(cfg-snmp)#**show history** [*<1-65535>*]	This displays configuration information about history group.
zte(cfg-snmp)#**show rmon**	This displays RMON status.
zte(cfg-snmp)#**show statistics** [*<1-65535>*]	This displays configuration information about statistic group.

RMON Configuration Example

The following examples describe how to set event 2, history 2, alarm 2 and statistics 1 respectively.

```
zte(cfg-snmp)#set event 2 description It'sJustForTest!!
zte(cfg-snmp)#set event 2 type logandtrap
```

```
zte(cfg-snmp)#set event 2 community public
zte(cfg-snmp)#set event 2 owner zteNj
zte(cfg-snmp)#set event 2 status valid

zte(cfg-snmp)#set history 2 datasource 16
zte(cfg-snmp)#set history 2 bucket 3
zte(cfg-snmp)#set history 2 interval 10
zte(cfg-snmp)#set history 2 owner zteNj
zte(cfg-snmp)#set history 2 status valid

zte(cfg-snmp)#set rmon enable

zte(cfg-snmp)#set alarm 2 interval 10
zte(cfg-snmp)#set alarm 2 variable 1.3.6.1.2.1.16.2.2.1.6.2.1
zte(cfg-snmp)#set alarm 2 sample absolute
zte(cfg-snmp)#set alarm 2 startup rising
zte(cfg-snmp)#set alarm 2 threshold 8 eventindex 2 rising
zte(cfg-snmp)#set alarm 2 threshold 15 eventindex 2 falling
zte(cfg-snmp)#set alarm 2 owner zteNj
zte(cfg-snmp)#set alarm 2 status valid

zte(cfg-snmp)#set statistics 1 datasource 16
zte(cfg-snmp)#set statistics 1 owner zteNj
zte(cfg-snmp)#set statistics 1 status valid
```

View configuration information about event 2:

```
zte(cfg-snmp)#show event 2
  EventIndex  : 2             Type       : log-and-trap
  Community   : public        Status     : valid
  Owner       : zteNj
  Description   :It'sJustForTest!!
```

View configuration information about history 2:

```
zte(cfg-snmp)#show history 2
  ControlIndex : 2               BucketsRequest: 3
  Interval     : 10              BucketsGranted: 3
  ControlStatus: valid           ControlOwner  : zteNj
  DataSource   : 1.3.6.1.2.1.2.2.1.1.16
```

View configuration information about alarm 2:

```
zte(cfg-snmp)#show alarm 2
  AlarmIndex   : 2       SampleType: absolute
  Interval     : 10      Value     : 16
  Threshold(R) : 8       Startup   : risingAlarm
  Threshold(F) : 15      Status    : valid
  EventIndex(R): 2       Variable  : 1.3.6.1.2.1.16.2.2.1.6.2.1
  EventIndex(F): 2       Owner     : zteNj
```

View configuration information about statistics 1:

```
zte(cfg-snmp)#show statistics 1
  StatsIndex: 1
  DropEvents    : 0   BroadcastPkts       : 0
  Octets        : 0   MulticastPkts       : 0
  Pkts          : 0   Pkts64Octets        : 0
  Fragments     : 0   Pkts65to127Octets   : 0
  Jabbers       : 0   Pkts128to255Octets  : 0
  Collisions    : 0   Pkts256to511Octets  : 0
  CRCAlignErrors: 0   Pkts512to1023Octets : 0
  UndersizePkts : 0   Pkts1024to1518Octets: 0
  OversizePkts  : 0   DataSource(port) : 1.3.6.1.2.1.2.2.1.1.16
  Status        : valid    Owner          : zteNj
```

After the above configuration, when the number of etherHistoryPkts of the first bucket of port 16 rises over 8 or the number falls below 15, the event with the index of 2 is triggered. The event with the index of 2 sends a trap to the management station, and creates a log simultaneously. This log can be viewed in the logTable of the event group.

Cluster Management

Cluster Management Overview

ZGMP is ZTE Group Manage Protocol. A cluster is a combination consisting of a set of switches in a specific broadcast domain. This set of switches forms a unified management domain, providing an external public network IP address and management interface, as well as the ability to manage and access each member in the cluster.

The management switch which is configured with a public network IP address is called a command switch. Other switches serve as member switches. In normal cases, a member switch is not configured with a public network IP address. A private address is allocated to each member switch through the class DHCP function of the command switch. The command switch and member switches form a cluster (private network).

It is recommended that you isolate the broadcast domain between the public network and the private network on the command switch and shield direct access to the private address. The command switch provides an external management and maintenance channel to manage the cluster in a centralized manner.

In general, the broadcast domain where a cluster is located consists of switches in these roles: Command switch, member switches, candidate switches and independent switches.

One cluster has only one command switch. The command switch can automatically collect the device topology and set up a cluster. After a cluster is set up, the command switch provides a cluster management channel to manage member switches. Member switches serve as candidate switches before they join the cluster. The switches that do not support cluster management are called independent switches.

Figure 83 shows the cluster management networking.

FIGURE 83 CLUSTER MANAGEMENT NETWORKING

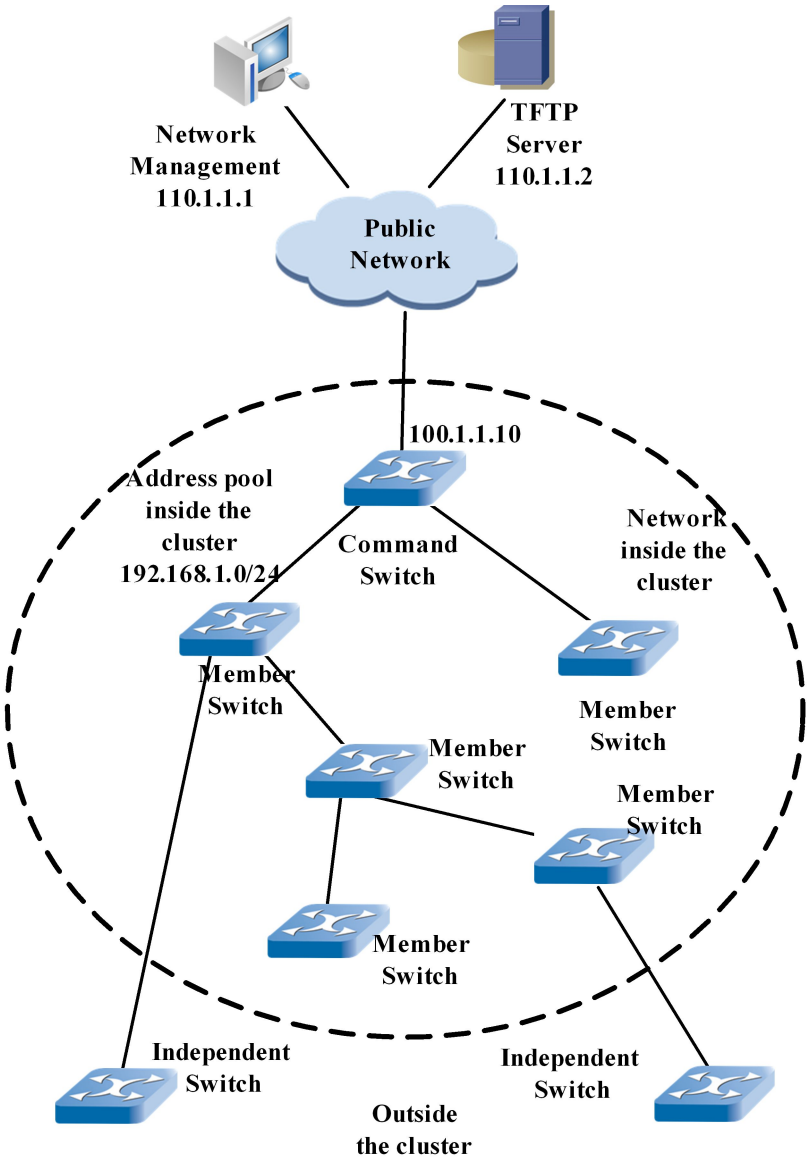
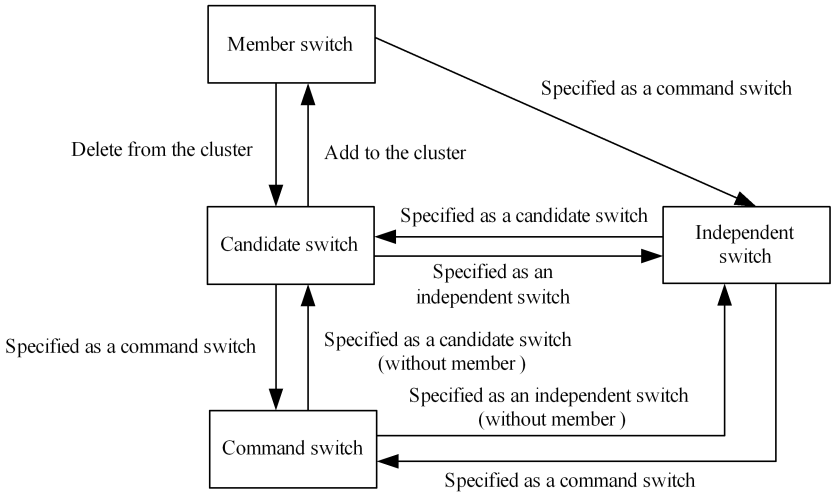


Figure 84 shows the changeover rule of the four roles of switches within a cluster.

FIGURE 84 SWITCH ROLE CHANGEOVER RULE


Member switch
Specified as a command switch
Delete from the cluster
Add to the cluster
Specified as a candidate switch
Candidate switch
Independent switch
Specified as an independent switch
Specified as a command switch
Specified as a candidate switch (without member)
Specified as an independent switch (without member)
Command switch
Specified as a command switch

Configuring ZDP

ZDP (Discovery Protocol) is a protocol used to discover the related information about the direct neighbor node, including the adjacent device ID, device type, version and port information. This protocol supports the refreshing and aging of the neighbor device information table.

The ZDP configuration on the switch includes the following contents:

Command	Function
`zte(cfg)#`**config group**	This enters cluster management configuration mode.
`zte(cfg-group)#`**set zdp** {**enable**|**disable**}	This enables/disables the system ZDP function.
`zte(cfg-group)#`**set zdp port** <*portlist*>{**enable**|**disable**}	This enables/disables the port ZDP function.
`zte(cfg-group)#`**set zdp trunk** <*trunklist*>{**enable**|**disable**}	This enables/disables the trunk ZDP function.
`zte(cfg-group)#`**set zdp holdtime** <*10-255*>	This sets the valid time for holding ZDP information. The unit is second, the default is 180s.
`zte(cfg-group)#`**set zdp timer** <*5-255*>	This sets the time interval for sending ZDP packets. The unit is second, the default is 30s.

Command	Function
zte(cfg)#**show zdp**	This displays the ZDP configuration.
zte(cfg)#**show zdp neighbour** [**detail**]	This displays the neighbor device information table.

Configuring ZTP

The topology protocol (ZTP) is a protocol used to collect network topology information. With the neighbor device information table collected through ZDP, ZTP sends and forwards ZTP topology collection packets through the relevant port in the specified VLAN to collect the topology information in the network (hop count) within a specific range and to create a topology information table which is used for knowing network topology status and managing the cluster.

The ZTP configuration on the switch includes the following contents:

Command	Function
zte(cfg)#**config group**	This enters cluster management configuration mode.
zte(cfg-group)#**set ztp** {**enable**|**disable**}	This enables/disables the system ZTP function.
zte(cfg-group)#**set ztp port** <*portlist*>{**enable**|**disable**}	This enables/disables the port ZTP function.
zte(cfg-group)#**set ztp trunk** <*trunklist*>{**enable**|**disable**}	This enables/disables the trunk ZTP function.
zte(cfg-group)#**ztp start**	This starts collecting topology information.
zte(cfg-group)#**set ztp vlan** <*1-4094*>	This configures a VLAN for collecting topology information.
zte(cfg-group)#**set ztp hop** <*1-128*>	This sets the range (hop count) of collecting topology information.
zte(cfg-group)#**set ztp timer** <*0-60*>	This sets time interval for collecting topology information periodically.

Command	Function
zte(cfg-group)#**set ztp hopdelay** *<1-1000>*	This sets the hop delay for forwarding topology requests.
zte(cfg-group)#**set ztp portdelay** *<1-100>*	This sets the port delay for forwarding topology requests.
zte(cfg)#**show ztp**	This displays ZTP configuration.
zte(cfg)#**show ztp mac** *<HH.HH.HH.HH.HH.HH>*	This displays detail information of specified device according to MAC address.
zte(cfg)#**show ztp device** [*<idlist>*]	This displays the configuration information of ZTP according to the device ID.

Configuring Cluster

After specifying the command switch, network topology information is got by ZDP/ZTP. Consequently, the cluster management and monitoring are implemented. Unique ID of a cluster consists of VLAN where cluster is located and MAC address of command switch.

Command	Function
zte(cfg)#**config group**	This enters cluster management configuration mode.
zte(cfg-group)#**set group candidate**	This configures a switch as candidate switch.
zte(cfg-group)#**set group independent**	This configures a switch as independent switch.
zte(cfg-group)#**set group commander ipport** *<0-63>*[**ip-pool** *<A.B.C.D/M>*]	This sets a command switch, specifies a layer 3 port number for cluster management and sets IP address pool for user cluster management.
zte(cfg-group)#**set group add mac** *<HH.HH.HH.HH.HH.HH><1-255>*	This adds a member based on device MAC address and specifies member ID number.

Command	Function
zte(cfg-group)#**set group add device** *<idlist>*	This adds a member based on temporary device ID obtained from collected topology information.
zte(cfg-group)#**set group delete member** *<idlist>*	This deleted a device with specified member ID from cluster.
zte(cfg-group)#**set group name** *<name>*	This sets cluster name.
zte(cfg-group)#**set group handtime** *<1-300>*	This sets a time interval for handshake between command switch and member switch.
zte(cfg-group)#**set group holdtime** *<1-300>*	This sets effective holding time of information about switches in cluster.
zte(cfg-group)#**set group syslogsvr** *<A.B.C.D>*	This sets IP address of internal public SYSLOG Server of cluster.
zte(cfg-group)#**set group tftpsvr** *< A.B.C.D >*	This sets IP address of internal public TFTP Server of cluster
zte(cfg-group)#**set group commander mac** {*<HH.HH.HH>*|*<HH.HH.HH.HH.HH.HH >*}*<vid>*	This configures MAC address of cluster commander switch. 00.d0.d0 is required to add on the front of MAC address.
zte(cfg-group)#**set group mac-mode standard**	This configures the protocol broadcast address mode of cluster management as standard mode.
zte(cfg-group)#**set group mac-mode extend** [**mac** *<HH.HH.HH.HH.HH.HH>*]	This configures the protocol broadcast address mode of cluster management as extended mode.
zte(cfg-group)#**erase member** {*<idlist>*|**all**}	This deletes configuration of specified member switch.
zte(cfg-group)#**reboot member** {*<idlist>*|**all**}	This restarts a specified member switch.
zte(cfg-group)#**save member** {*<idlist>*|**all**}	This saves configuration of specified member switch.

Command	Function
zte(cfg)#**show group**	This displays cluster configuration information.
zte(cfg)#**show group candidate**	This displays candidate switches information.
zte(cfg)#**show group member** [*<1-255>*]	This displays cluster member switches information.

Cluster Management Configuration Example

As shown in figure CLUSTER MANAGEMENT NETWORKING, the initial configuration of the switches is the default configuration. Here, set the VLAN where the public network IP address of the command switch in the cluster is located to 2525, the IP address to 100.1.1.10/24, the gateway address to 100.1.1.1, the cluster management VLAN to 4000, the private address pool to 192.168.1.0/24, and the IP address of the TFTP Server of the whole cluster to 110.1.1.2.

The detailed configuration is as follows:

1. Configure the public network IP address of the command switch and the gateway.

```
WYXX(cfg)#set vlan 2525 enable
WYXX(cfg)#set vlan 2525 add port 1-16 tag

WYXX(cfg)#config router
WYXX(cfg-router)#set ipport 25 ipaddress 100.1.1.10/24
WYXX(cfg-router)#set ipport 25 vlan 2525
WYXX(cfg-router)#set ipport 25 enable

WYXX(cfg-router)#iproute 0.0.0.0/0 100.1.1.1
```

2. Create a cluster on layer 3 port 1 of the command switch and VLAN 1 (default VLAN).

```
WYXX(cfg)#config group
WYXX(cfg-group)#set group commander ipport 1
 ip-pool 192.168.1.1/24

Cmdr.WYXX(cfg-group)#ztp start
Cmdr.WYXX(cfg-group)#show ztp device
  Last collection vlan : 1
  Last collection time : 188 ms
   Id   MacAddress       Hop   Role   HostName  Platform
  ------------------------------------------------------------
    0  00.d0.d0.fc.08.6c      0  cmdr     zte    ZXR10 2926
    1  00.d0.d0.fc.08.d6      1  candi    zte    ZXR10 2909
    2  00.d0.d0.fc.08.c3      1  candi    zte    ZXR10 2918
    3  00.d0.d0.fc.08.f5      2  candi    zte    ZXR10 2918
    4  00.d0.d0.fc.08.d5      2  candi    zte    ZXR10 2926
    5  00.d0.d0.fc.09.3a      1  candi    zte    ZXR10 2818S

Cmdr.WYXX(cfg-group)#set group add device 1-5
  Adding device id : 1   ...  Successed to add member!
  Adding device id : 2   ...  Successed to add member!
  Adding device id : 3   ...  Successed to add member!
  Adding device id : 4   ...  Successed to add member!
```

```
  Adding device id : 5   ...  Successed to add member!

Cmdr.WYXX(cfg-group)#show group member
  MbrId MacAddress        IpAddress          Status
  ----- ----------------- ----------------- -------
  1     00.d0.d0.fc.08.d6 192.168.1.2/24      Up
  2     00.d0.d0.fc.08.cf 192.168.1.3/24      Up
  3     00.d0.d0.fc.08.fa 192.168.1.4/24      Up
  4     00.d0.d0.fc.08.d5 192.168.1.5/24      Up
  5     00.d0.d0.fc.09.3a 192.168.1.6/24      Up
```

3. Switch to each member switch and add all ports to VLAN 4000 (taking member 4 as an example).

```
Cmdr.WYXX(cfg)#set vlan 4000 enable
Cmdr.WYXX(cfg)#set vlan 4000 add port 1-16 tag

Cmdr.WYXX(cfg)#rlogin member 4
  Trying  ...Open
  Connecting ...

Membr_4.zte>enable

Membr_4.zte(cfg)#set vlan 4000 enable
Membr_4.zte(cfg)#set vlan 4000 add port 1-16 tag
```

4. Delete the cluster created on VLAN 1.

```
Cmdr.WYXX(cfg-group)#set group delete member 1-5
  Deleting member id : 1   ...  Successed to del member!
  Deleting member id : 2   ...  Successed to del member!
  Deleting member id : 3   ...  Successed to del member!
  Deleting member id : 4   ...  Successed to del member!
  Deleting member id : 5   ...  Successed to del member!

Cmdr.WYXX(cfg-group)#set group candidate
WYXX(cfg-group)#
```

5. Create a cluster on VLAN 4000.

```
WYXX(cfg-group)#set ztp vlan 4000

WYXX(cfg-group)#set group commander ipport 1
ip-pool 192.168.1.1/24

Cmdr.WYXX(cfg-group)#ztp start
Cmdr.WYXX(cfg-group)#show ztp device
  Last collection vlan : 4000
  Last collection time : 176 ms
   Id  MacAddress       Hop   Role  HostName     Platform
  ---  ---------------  ---  -----  ---------  ----------
    0  00.d0.d0.fc.08.6c    0  cmdr     zte   ZXR10 2926
    1  00.d0.d0.fc.08.d6    1  candi    zte   ZXR10 2909
    2  00.d0.d0.fc.08.cf    1  candi    zte   ZXR10 2918
    3  00.d0.d0.fc.08.fa    2  candi    zte   ZXR10 2918
    4  00.d0.d0.fc.08.d5    2  candi    zte   ZXR10 2926
    5  00.d0.d0.fc.09.3a    3  candi    zte   ZXR10 2918s

Cmdr.WYXX(cfg-group)#set group add device 1-5
  Adding device id : 1   ...  Successed to add member!
  Adding device id : 2   ...  Successed to add member!
  Adding device id : 3   ...  Successed to add member!
  Adding device id : 4   ...  Successed to add member!
  Adding device id : 5   ...  Successed to add member!

Cmdr.WYXX(cfg-group)#show group member
  MbrId MacAddress        IpAddress          Status
  ----- ----------------- ----------------- ----------
  1     00.d0.d0.fc.08.d6 192.168.1.2/24      Up
  2     00.d0.d0.fc.08.cf 192.168.1.3/24      Up
  3     00.d0.d0.fc.08.fa 192.168.1.4/24      Up
  4     00.d0.d0.fc.08.d5 192.168.1.5/24      Up
  5     00.d0.d0.fc.09.3a 192.168.1.6/24      Up
```

6. Set the IP address of the TFTP Server in the cluster to 110.1.1.2.

```
Cmdr.WYXX(cfg-group)#set group tftpsvr 110.1.1.2
```

7. Download version kernel.Z on member 4.

```
Membr_4.zte(cfg-tffs)#tftp commander download kernel.Z
```

SFLOW

SFLOW Overview

SFLOW is a technique to monitor high speed data transmission network. It uses SFLOW proxy embedded in network equipments to send the sampled data packets to the SFLOW collectors.

SFLOW implements the following functions:

- Provide the correct statistics about client flow.
- Monitor intrusion and police violation to make the network more safer.
- Monitor the network traffic and application visually.
- Provide the correct data suitable for capacity deployment.
- Ensure the priority of traffic across core network.
- Recognize the network application flow from the remote site to ensure the effect on server.

Basic Configuration of SFLOW

To configure SFLOW, perform the following steps.

Command	Function
`zte(cfg)#`**set sflow ingress feport** *<feportlist>*{ **off** | **on** { **frequency** *<2-16000000 >*}}	This configures sampling rate on ingress direction of 100M port.
`zte(cfg)#`**set sflow** {**ingress** | **egress** } **geport***<geportlist>*{**off** | **on** { **frequency** *<20000-100000001>*}}	This configures sampling rate on ingress/egress direction of gigabit port.
`zte(cfg)#`**set sflow** {**ingress** | **egress** }{**cpu** | **continuous**}	This configures SFLOW sample frequency reload-mode on ingress or egress direction of gigabit port.
`zte(cfg)#`**set sflow ingress geport sample-mode** { **all** | **forward** }	This configures ingress sample mode of SFLOW function on gigabit port.

Command	Function
zte(cfg)#**set sflow agent-address** *<A.B.C.D>*	This sets proxy IP address of SFLOW.
zte(cfg)#**set sflow collector-address** *<A.B.C.D>*	This sets IP address of SFLOW collector.

WEB

WEB Overview

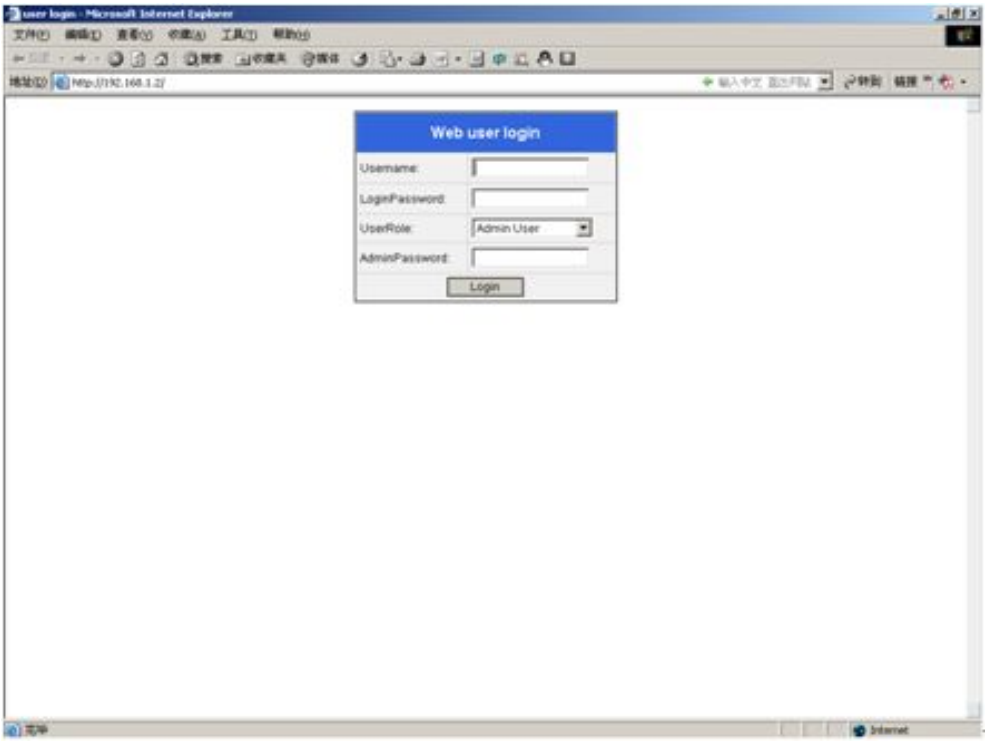
ZXR10 2900 provides a embedded Web server stored in flash memory, which allows user to use a standard Web browser (it is recommended to use IE4.0 above and 1024×768 resolution) for managing remote switch.

Configuring System Login

On the condition that WEB connection has been configured on the switch (refer to Configuration through WEB Connection):

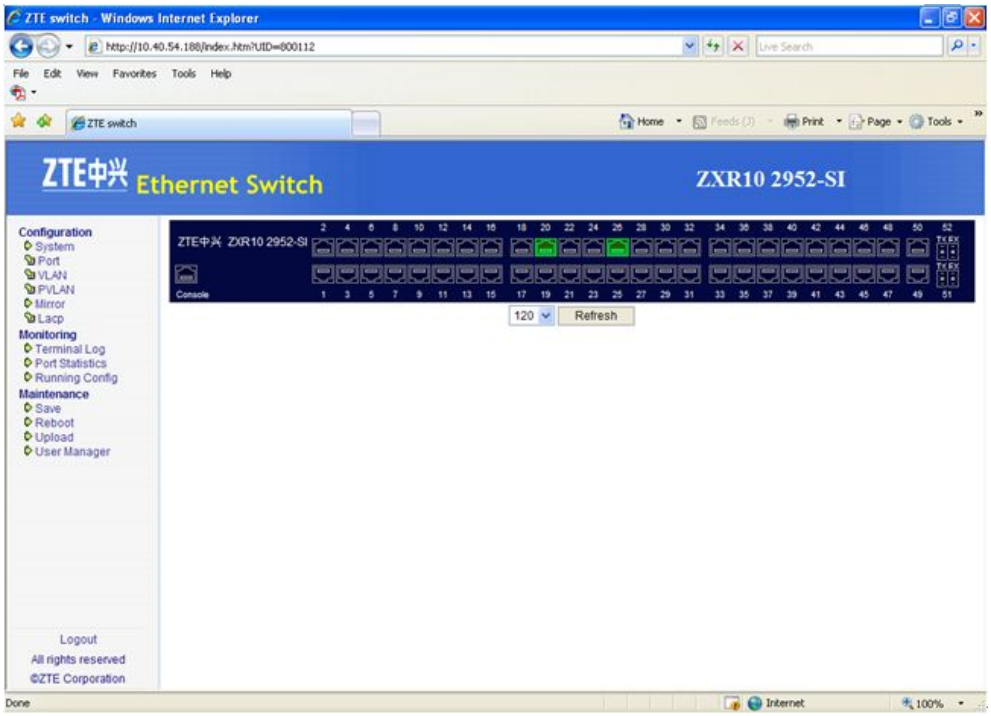
1. Open Microsoft Internet Explore.
2. Enter IP address of switch in URL (this address is that switch can connect), press the button **Enter** to open system login interface, as shown in Figure 85.

FIGURE 85 SYSTEM LOGIN INTERFACE



3. Enter legal username and password, select user privilege. Admin user need enter login password and management password. Guest user only need enter login password. Click **Login** button to login in to system main interface, as shown in Figure 86.

FIGURE 86 SYSTEM MAIN INTERFACE

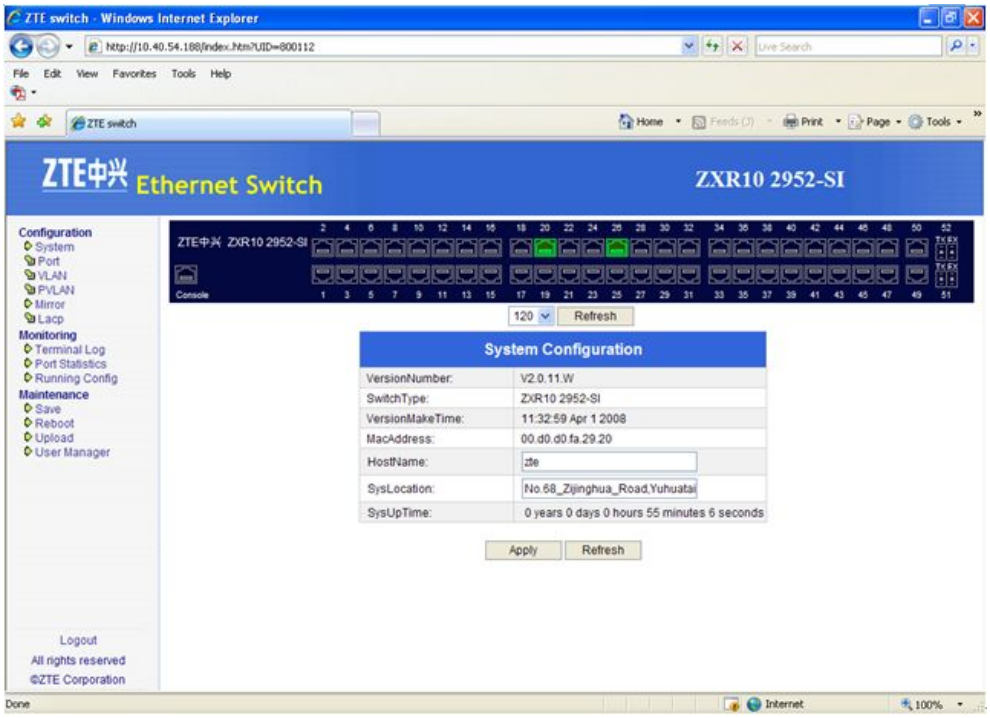


Configuration Management

System Information

Click directory tree on the left of system main page, **Configuration > System**, open system information page (by default, Configuration directory is expansive), as shown in Figure 87.

FIGURE 87 SYSTEM INFORMATION PAGE



This page displays the following system information:

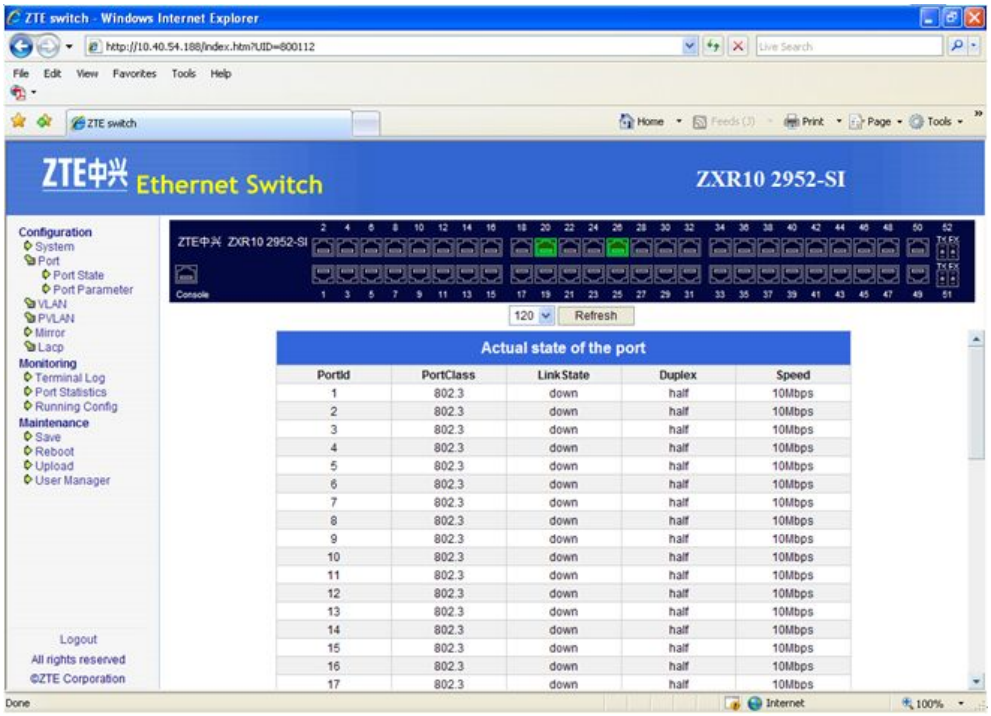
- [VersionNumber]: version number
- [SwitchType]: switch type
- [VersionMakeTime]: version making time
- [MacAddress]: switch hardware address
- [Module_1]: information of extended card 1
- [HostName]: system name
- [SysLocation]: system location
- [SysUpTime]: the running time after the system is started.

Both "HostName"and "SysLocation"can be configured. After configuration, click the **Apply** button to submit to complete the configuration.

Port Management

1. Click directory tree on the left of system main page, **Configuration > Port > Port State**, open port state information page as shown in Figure 88 .

FIGURE 88 PORT STATE INFORMATION PAGE


ZTE switch - Windows Internet Explorer
ZTE中兴 Ethernet Switch
ZXR10 2952-SI
Configuration
System
Port
Port State
Port Parameter
VLAN
PVLAN
Mirror
Lacp
Monitoring
Terminal Log
Port Statistics
Running Config
Maintenance
Save
Reboot
Upload
User Manager
Logout
All rights reserved
©ZTE Corporation
120
Refresh
Actual state of the port
PortId | PortClass | LinkState | Duplex | Speed
1 | 802.3 | down | half | 10Mbps
2 | 802.3 | down | half | 10Mbps
3 | 802.3 | down | half | 10Mbps
4 | 802.3 | down | half | 10Mbps
5 | 802.3 | down | half | 10Mbps
6 | 802.3 | down | half | 10Mbps
7 | 802.3 | down | half | 10Mbps
8 | 802.3 | down | half | 10Mbps
9 | 802.3 | down | half | 10Mbps
10 | 802.3 | down | half | 10Mbps
11 | 802.3 | down | half | 10Mbps
12 | 802.3 | down | half | 10Mbps
13 | 802.3 | down | half | 10Mbps
14 | 802.3 | down | half | 10Mbps
15 | 802.3 | down | half | 10Mbps
16 | 802.3 | down | half | 10Mbps
17 | 802.3 | down | half | 10Mbps

This page displays the following information of port:

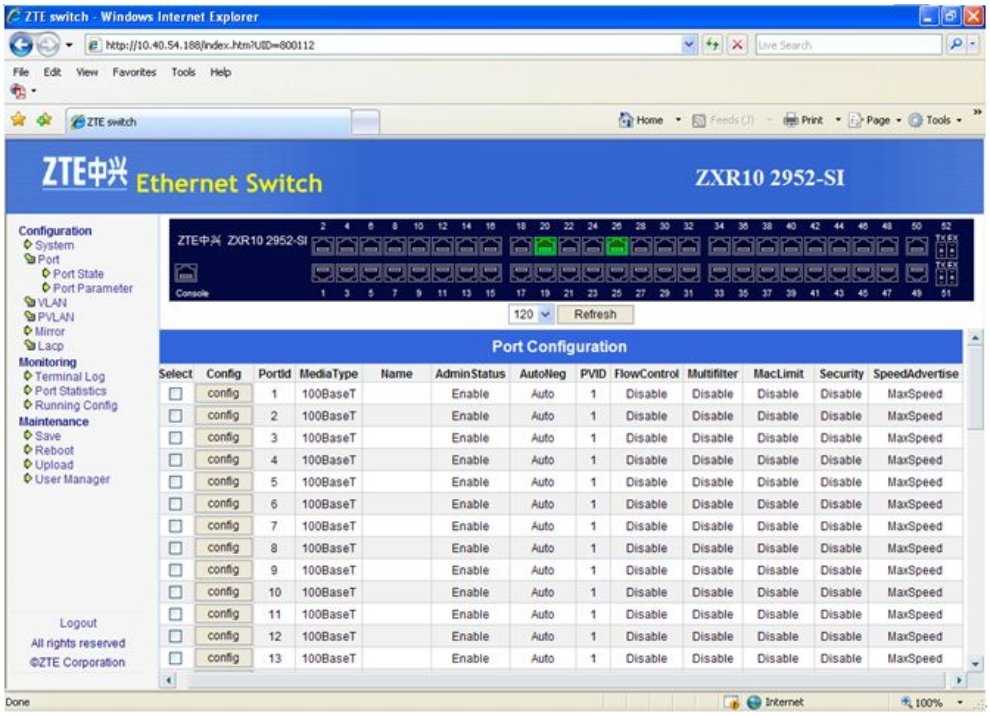
- [PortClass]: port class
- [LinkState]: port linkup|linkdown state
- [Duplex]: duplex working state of port
- [Speed]:working speed of port

Note:

Linkdown of port means that port hasn't physical connection. The displaying values of "Duplex" and "Speed" are meaningless.

2. Click directory tree on the left of main page, **Configuration > Port > Port Parameter**, open port configuration information page, as shown in Figure 89.

FIGURE 89 PORT CONFIGURATION INFORMATION PAGE

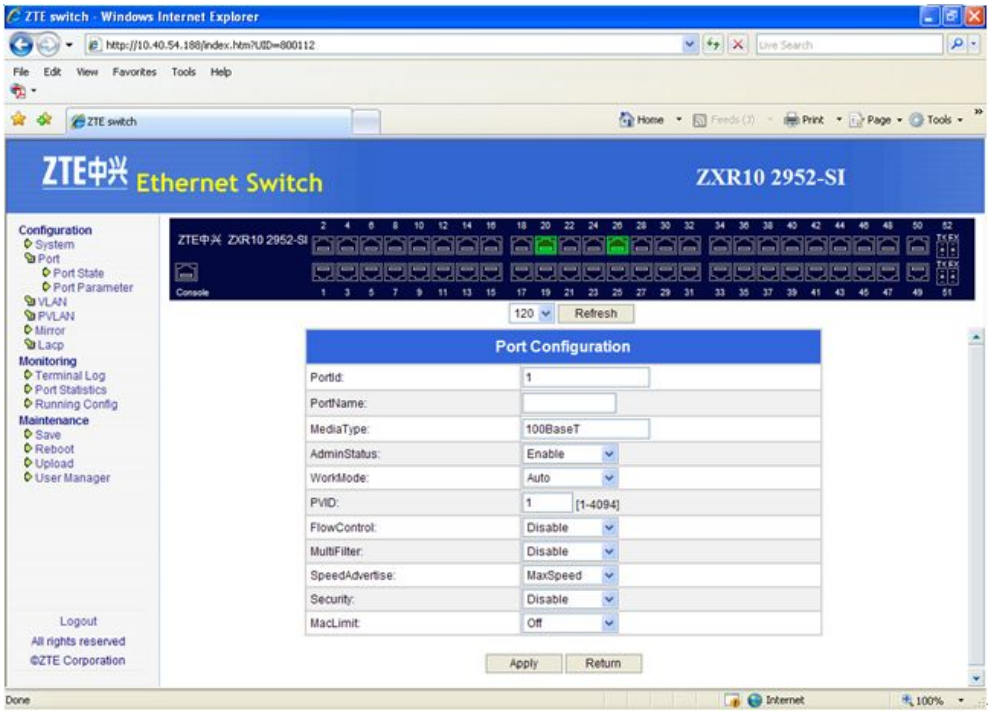

ZTE switch - Windows Internet Explorer
ZTE Ethernet Switch
ZXR10 2952-SI
Configuration
System
Port
Port State
Port Parameter
VLAN
PVLAN
Mirror
Lacp
Monitoring
Terminal Log
Port Statistics
Running Config
Maintenance
Save
Reboot
Upload
User Manager
Logout
All rights reserved
©ZTE Corporation
Refresh
Port Configuration
Select Config PortId MediaType Name AdminStatus AutoNeg PVID FlowControl MultiFilter MacLimit Security SpeedAdvertise
config 1 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 2 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 3 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 4 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 5 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 6 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 7 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 8 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 9 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 10 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 11 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 12 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed
config 13 100BaseT Enable Auto 1 Disable Disable Disable Disable MaxSpeed

This page displays the following information of port (refer to Port Basic Configuration):

- [MediaType]: port media type
- [PortName]: port name
- [AdminStaus]: port enable
- [AutoNeg]: port working mode, that is , working speed and duplex mode
- [PVID]: port default VLAN ID
- [FlowControl]: port flow control enable
- [MultiFilter]: port multicast filter enable
- [MacLimit]: port Mac address learning limit
- [Security]: port security enable
- [SpeedAdvertise]: port speed advertisement

3. Single port configuration: click the **Config** button in the line of port to be configured in port configuration information page list to open configuration page of this port, as shown in Figure 90.

FIGURE 90 SINGLE PORT CONFIGURATION PAGE



Configure the attribute of the selected port in this page, after configuration, click the **Apply** button to complete the configuration.

Note:

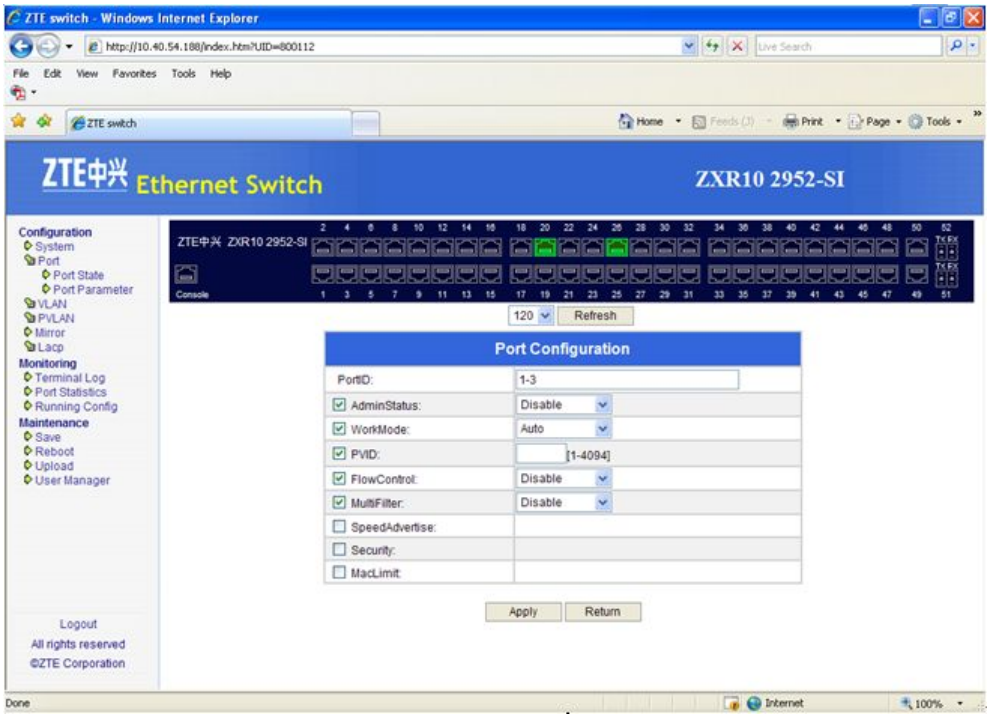
"Security" and "MacLimit" are conflicting. Therefore the two attributes can't be configured enabled at the same time.

Caution:

Note: If the port connects the network management host is shutdown network management will be interrupted.

4. Bulk port configuration: select multiple ports in port configuration information page listselect **Select All** to select all ports, and then click **Apply** to open bulk port configuration page, as shown in Figure 91.

FIGURE 91 BULK PORT CONFIGURATION PAGE

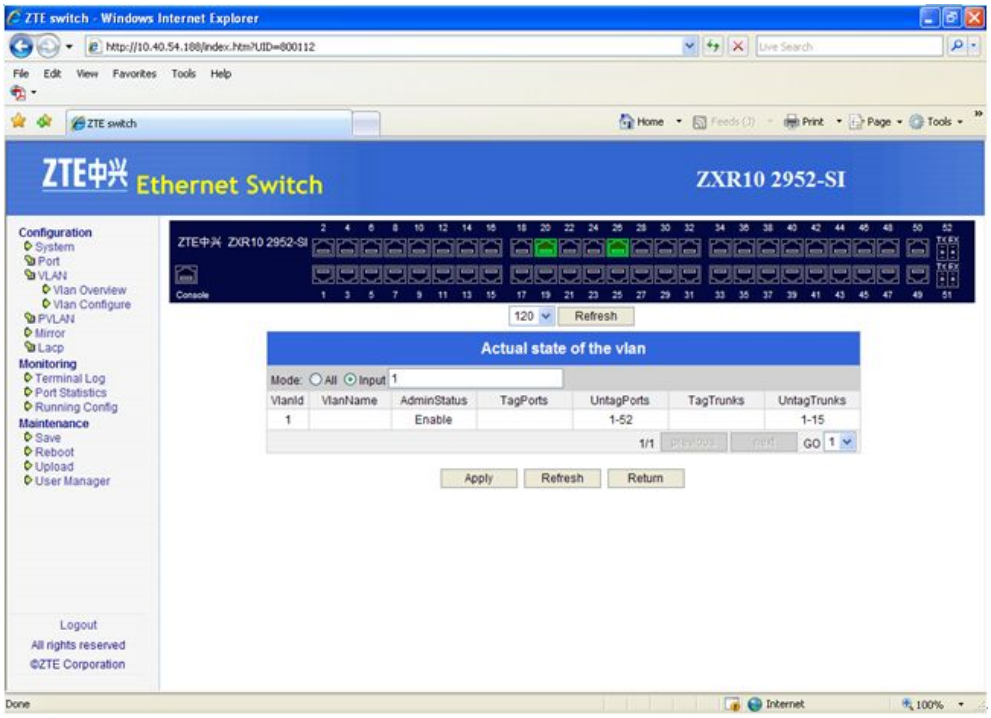


Click the check box before attribute to select the attribute to be configured in this page, and then click **Apply** to submit to complete the configuration.

VLAN Management

1. Click directory tree on the left of main page, **Configuration > VLAN > Vlan Overview**, open VLAN information page to display the VLAN information which is operated currently. If the VLAN hasn't been operated the default VLAN will be displayed. Refer to Figure 92.

FIGURE 92 VLAN INFORMATION PAGE



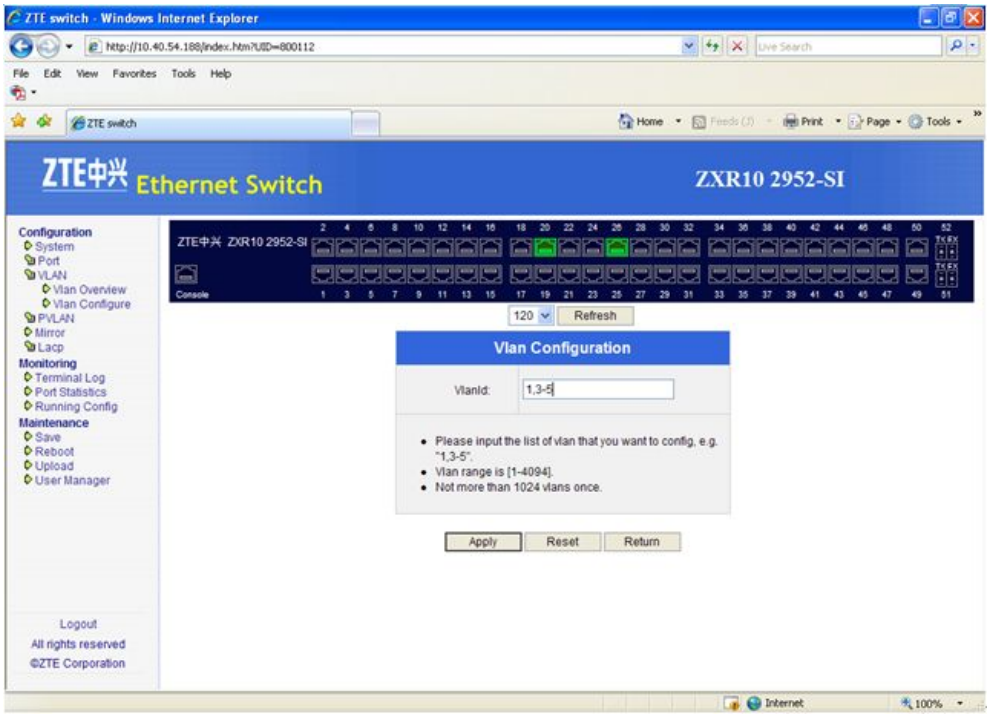
When VLAN entry to be displayed is more than 20, it will be displayed by page and page number will prompted at bottom right corner of page. When the number of page is more than one page, click **previous** or **next** to switch page or select page number in **GO** drop-down box.

This page displays the following information of VLAN:

- [VlanName]:VLAN name
- [AdminStatus]:VLAN enable
- [Tagged Ports]:port with tag in VLAN
- [Untagged Ports]:port without tag in VLAN
- [Tagged Trunks]:trunk with tag in VLAN
- [Untagged Trunks]:trunk without tag in VLAN

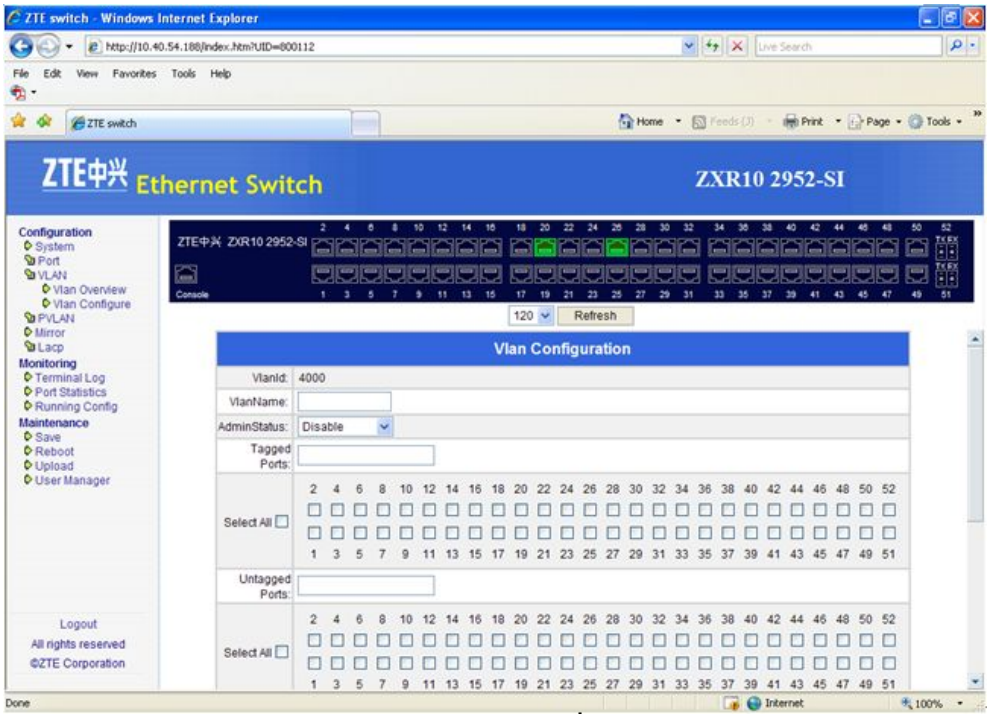
2. View specific VLAN information: select [Input] in VLAN information page, and then enter VLAN number in the following text box, such as "1,3-5" or select [All]. Click [Apply] to submit to get the corresponding VLAN information.
3. Click directory tree **Configuration > VLAN > Vlan Configure** on the left of main page, open VLAN number entering page, as shown in Figure 93.

FIGURE 93 VLAN NUMBER ENTERING PAGE



4. Enter VLAN number in VLAN number page(such as "1, 3-5"), click **Apply** to enter single VLAN configuration or bulk VLAN configuration page, respective description are as follows:
   - Figure 94 shows the single VLAN configuration interface.

FIGURE 94 SINGLE VLAN CONFIGURATION PAGE



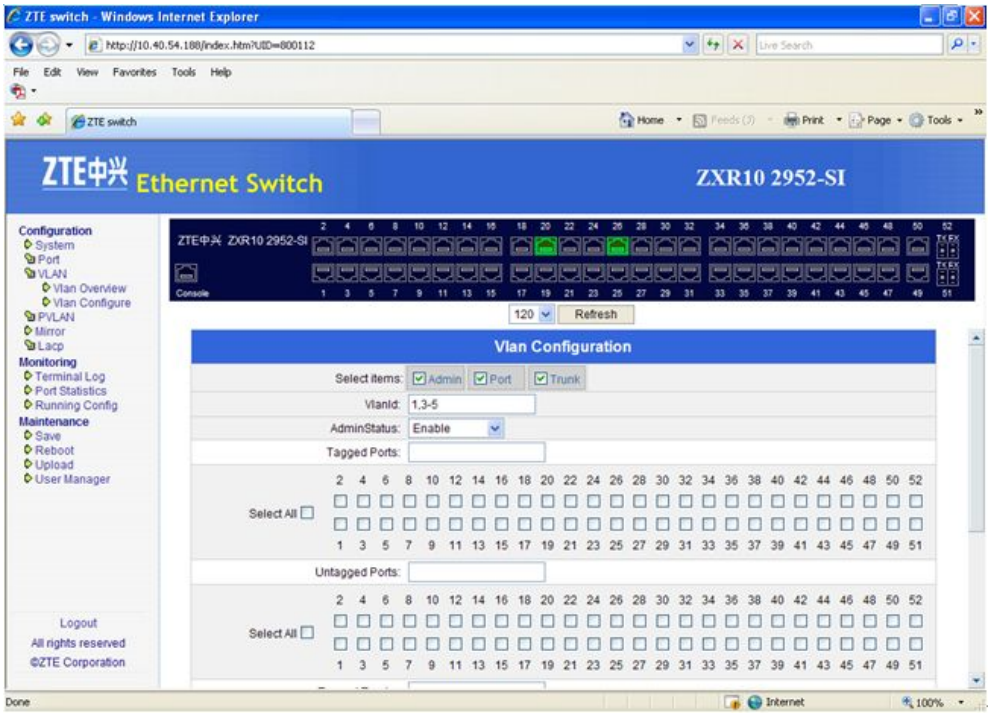
After setting some attributes of VLAN in this page, click **Apply** to complete the configuration.

Note:

When configuring port/Trunk in VLAN, enter port/Trunk number in the following text box, the format is as "1,3-5". Also can select the corresponding check box to add them into VLAN.

Figure 95 shows bulk VLAN configuration.

FIGURE 95 BULK VLAN CONFIGURATION PAGE



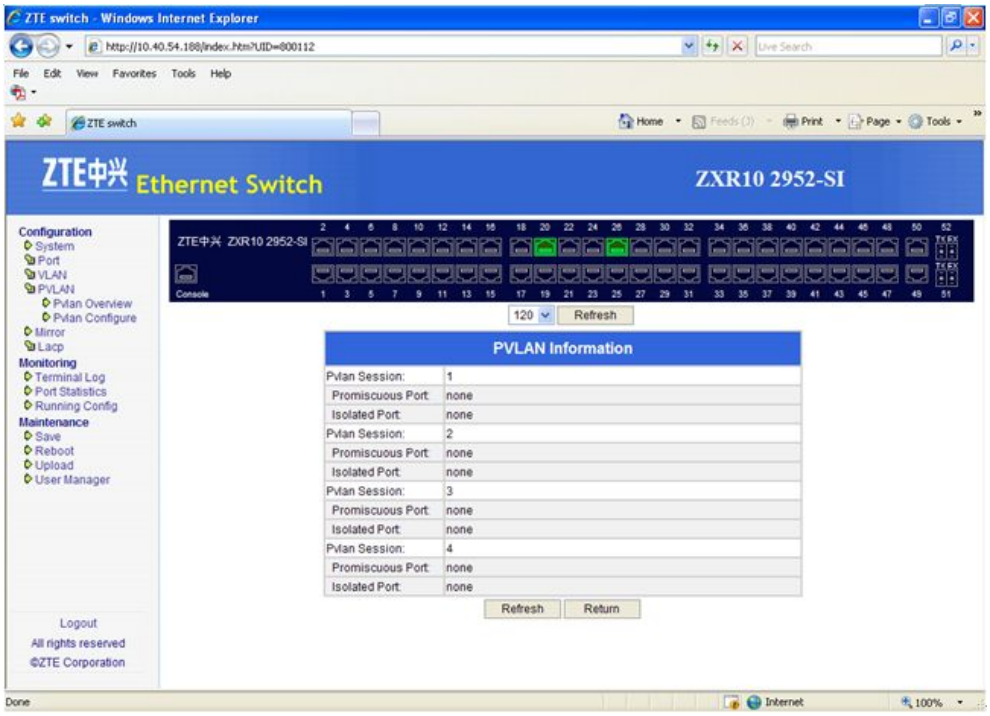
Admin of Select items is used to enable VLAN. Port is ordinary port of bulk VLAN configuration. Trunk is Trunk group of bulk VLAN configuration.

After setting some attributes of VLAN in this page, click **Apply** to complete the configuration.

PLAN Management

1. Click directory tree **Configuration > PVLAN > Pvlan Overview** on the left of main page, open PVLAN information page, as shown in Figure 96.

FIGURE 96 PVLAN INFORMATION PAGE

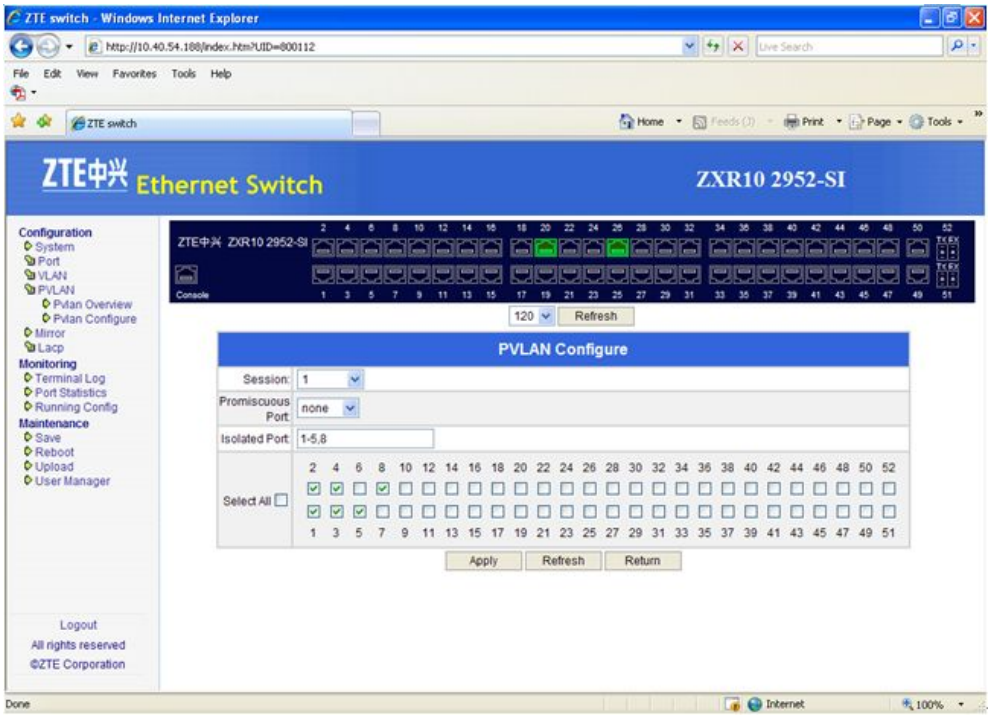


This page displays the following information of PVLAN:

- [pvlan Session]:PVLAN instance
- [Promiscuous Port]:shared port
- [Isolated Port]:isolated port

2. Click directory tree **Configuration > PVLAN > Pvlan Configure** on the left of main page, open PVLAN configuration page, as shown in Figure 97.

FIGURE 97 PVLAN CONFIGURATION PAGE



This page displays the following information of PVLAN:

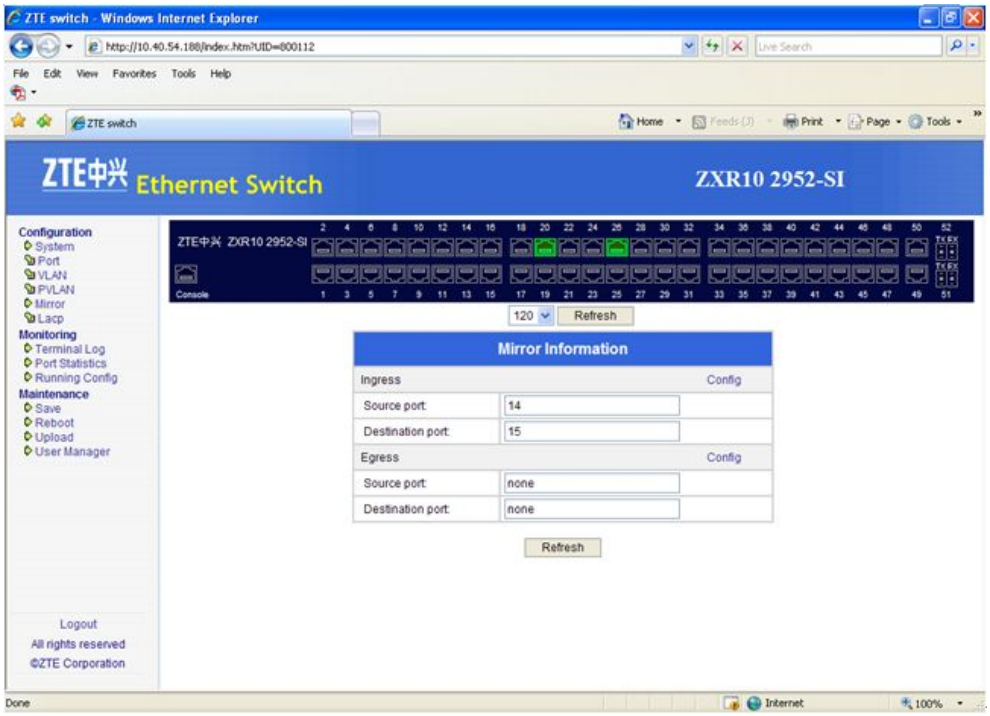
- [pvlan Session]:pvlan instance
- [Promiscuous Port]:shared port
- [Isolated Port]: isolated port

This page also can set attributes. After setting, click **Apply** to submit. When system is configured successfully, the configured information page will be displayed.

Port Mirroring Management

1. Click directory tree **Configuration > Mirror** on the left of main page, open Mirror information page, refer to Figure 98.

FIGURE 98 MIRROR INFORMATION PAGE

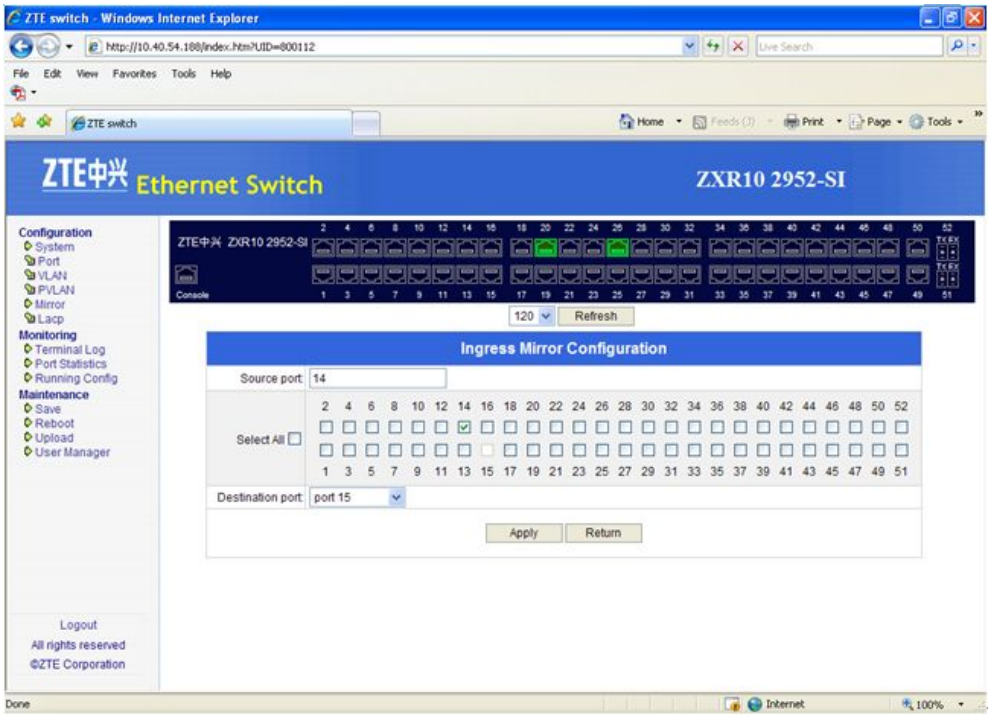


This page displays the following information of port mirroring (including ingress and egress)

- [Source port]:mirroring source port
- [Destination port]:mirroring destination port

2. Click **Config** on the right of Ingress column to open port ingress mirroring configuration page. Refer to Figure 99.

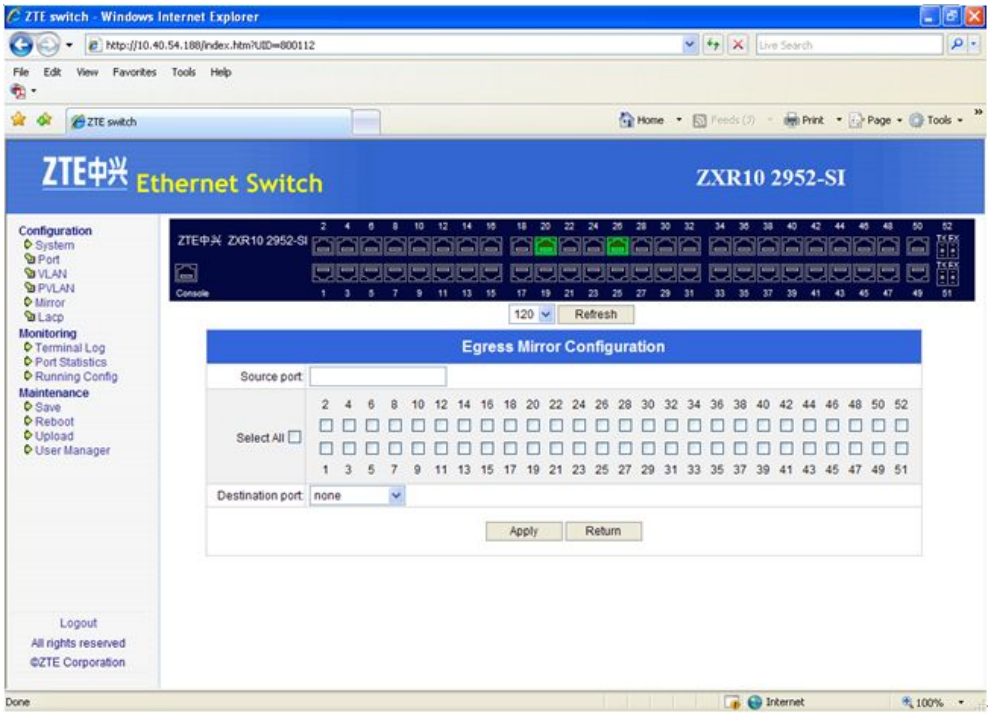
FIGURE 99 PORT INGRESS MIRRORING CONFIGURATION PAGE



Ingress source port, egress source port and destination port can be configured in this page. After setting, click **Apply** to submit to complete the configuration.

3. Click **Config** on the right of Egress column to open port egress mirroring configuration page, as shown in Figure 100.

FIGURE 100 PORT EGRESS MIRRORING CONFIGURATION PAGE

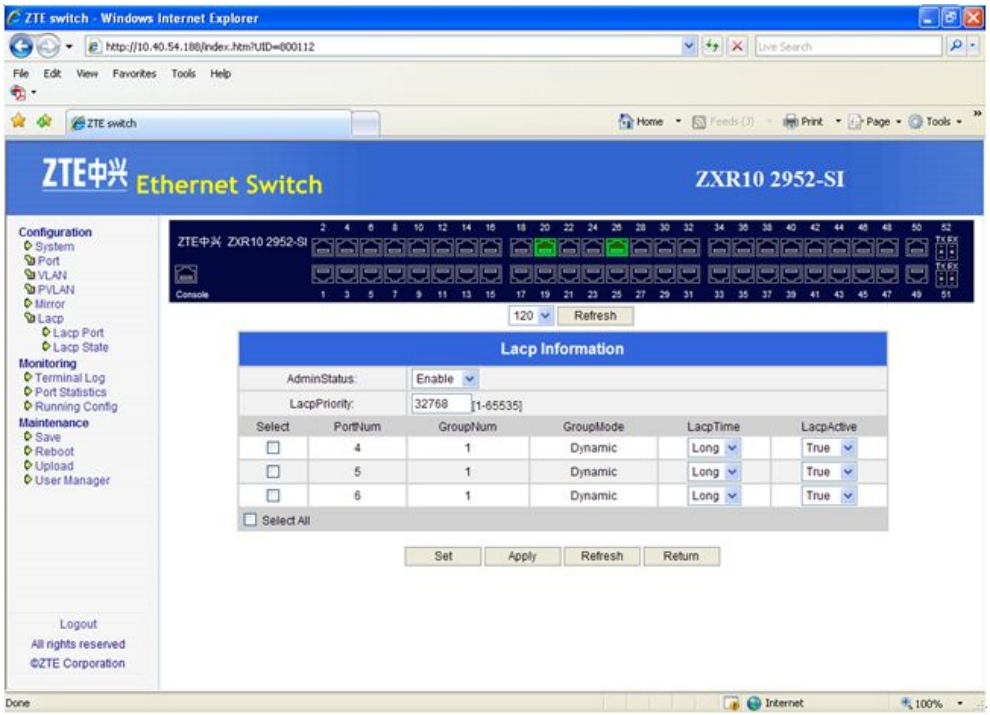


Egress mirroring source port and destination port can be configured in this page. After setting, click **Apply** to submit to complete the configuration.

LACP Management

1. Click directory tree **Configuration > Lacp > Lacp Port** on the left of main page, open LACP basic information page, as shown in Figure 101.

FIGURE 101 LACP BASIC ATTRIBUTE PAGE



The page information includes:

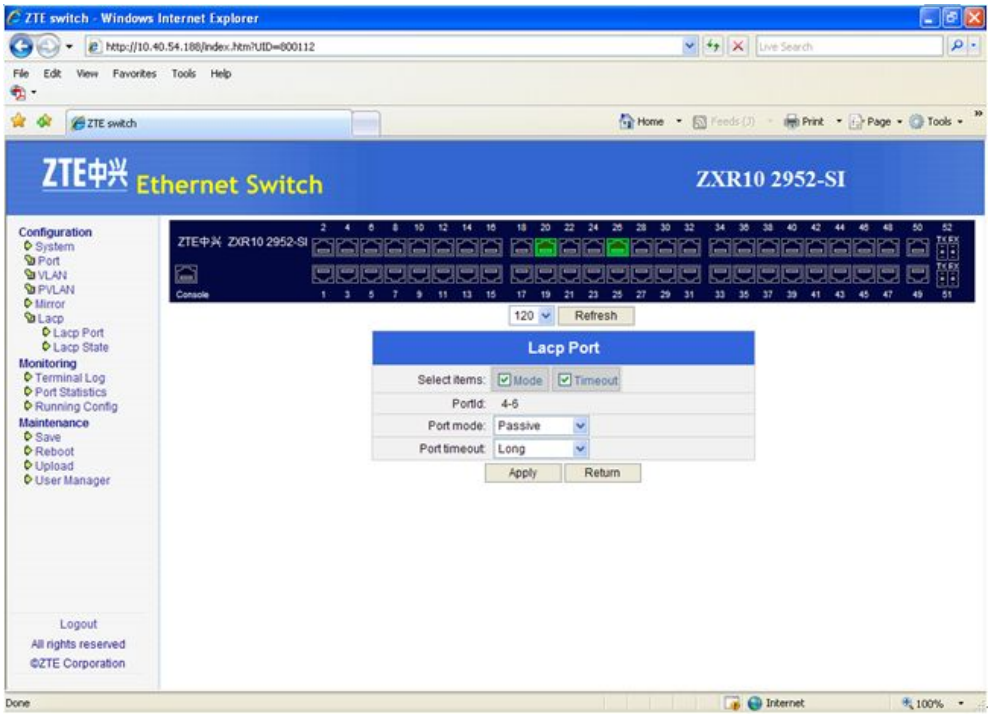
i. LACP basic information
   - [AdminStatus]:LACP enable
   - [LacpPriority]:LACP priority

ii. aggregation port information
   - [GroupNum]: aggregation group number that aggregation port belongs to
   - [GroupMode]: aggregation group aggregation mode that port belongs to
   - [LacpTime]: aggregation port timeout mode
   - [LacpActive]: aggregation port active/passive mode

set basic attributes of "AdminStatus" and "LacpPriority" in this page and set attributes of "LacpTime" and "LacpActive" of aggregation port. After setting, click **Apply** to submit to complete the configuration.

When setting same configuration of bulk aggregation port attribute , click the corresponding check box to select multiple aggregation ports (select **Select All** to select all ports), and then click **Set** to open configuration page of bulk aggregation port, as shown in Figure 102.

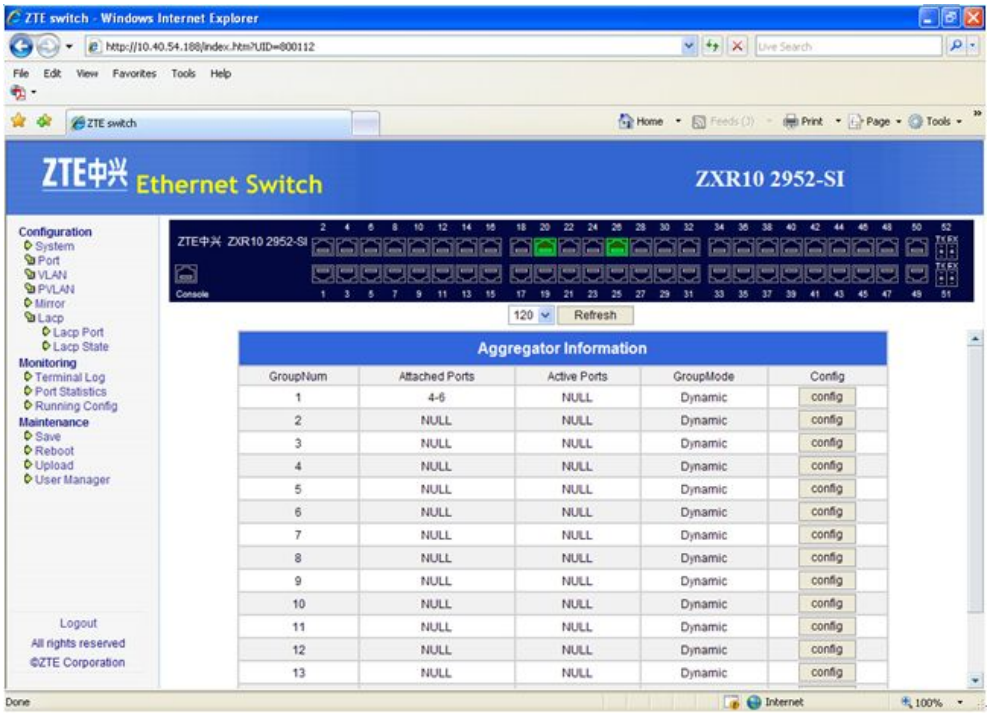
FIGURE 102 BULK AGGREGATION PORT CONFIGURATION PAGE



After setting attributes of aggregation port in this page, click **Apply** to submit.

2. Click directory tree **Configuration > Lacp > Lacp State** on the left of main page, open aggregation group information page, as shown in Figure 103.

FIGURE 103 AGGREGATION GROUP INFORMATION PAGE

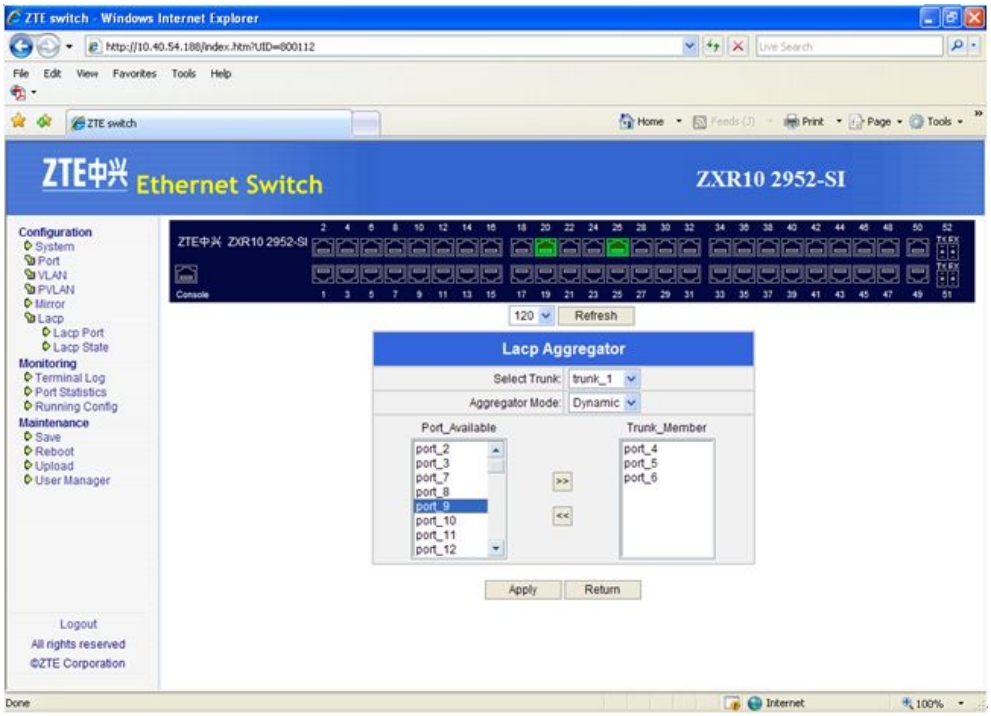


This page displays the following information of aggregation group:

- [Attached Ports]:attached ports in aggregation group
- [Active Ports]:active ports in aggregation group
- [GroupMode]:aggregation mode of aggregation group

Click **Config** of the right column to open the corresponding aggregation group configuration page, as shown in Figure 104.

FIGURE 104 AGGREGATION GROUP CONFIGURATION PAGE



Configure "Aggretator Mode" attribute of aggregation group in this page , bind port with aggregation group (select port in optional port column, click >>) and release port from aggregation group (select port in aggregation port column, click <<).

Note:

Only the ports with same attribute can be bound into the same aggregation group. Each aggregation group can bind up to 8 ports.

Caution:

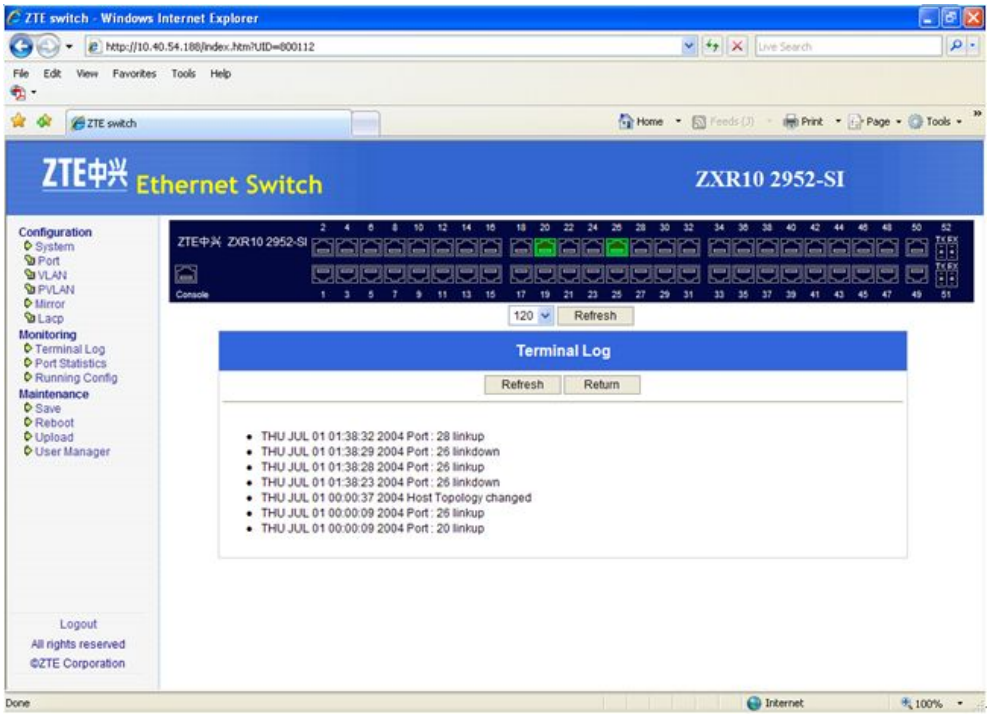
Note: avoid binding the port connects the network management host with aggregation group, or the network management will be interrupted

Monitor Information

Terminal Log

Click directory tree **Monitoring > Terminal Log** on the left of main page, open terminal log information page, as shown in Figure 105.

FIGURE 105 TERMINAL LOG INFORMATION PAGE

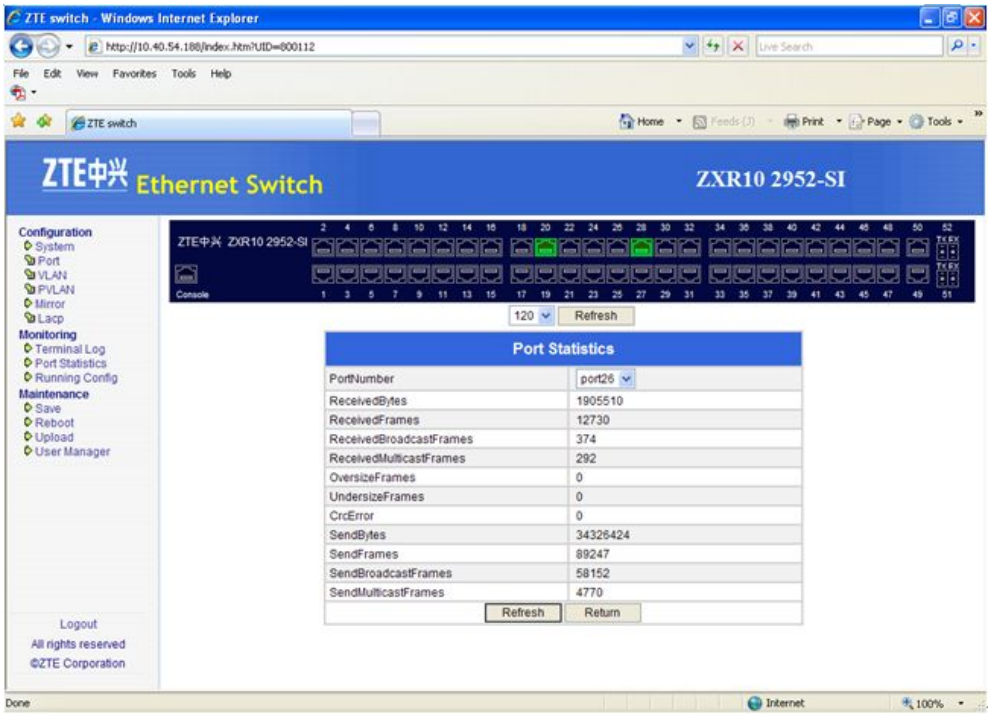


Click **Refresh** button to update terminal log information.

Port Statistics

Click directory tree **Monitoring > Port Statistics** on the left of main page, open port statistics information page, as shown in Figure 106.

FIGURE 106 PORT STATISTICS INFORMATION PAGE



Click **Refresh** button to update port statistics information.

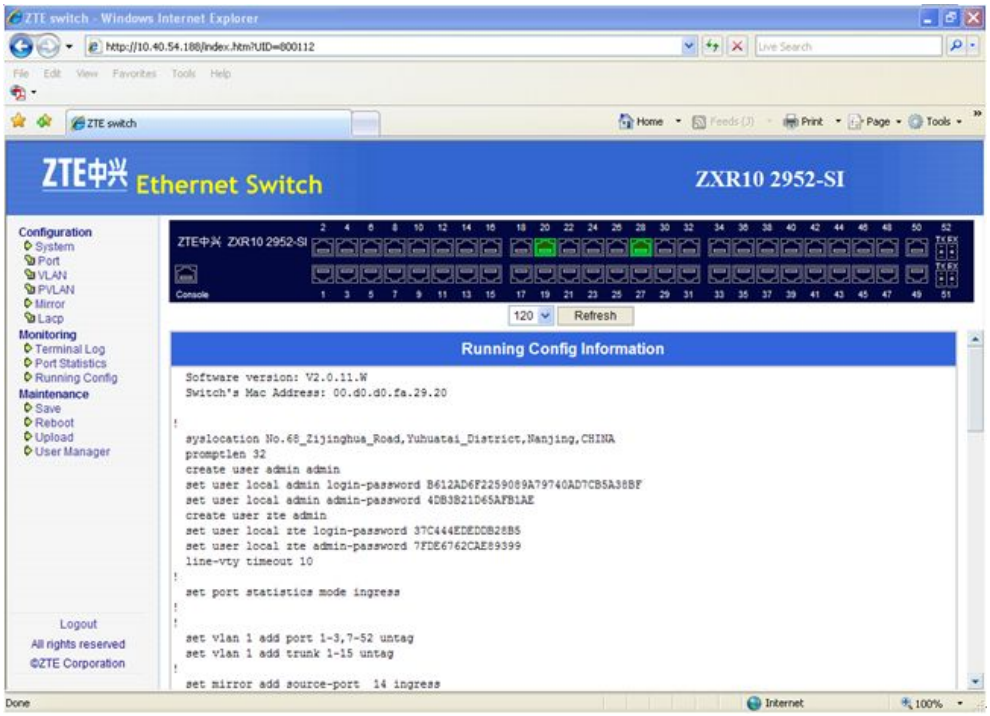
Select port in **PortNumber** drop-down box to get the port statistics. statistics includes:

- [ReceivedBytes]:Received bytes
- [ReceivedFrames]:Received frames
- [ReceivedBroadcastFrames]:Received broadcast frames
- [ReceivedMulticastFrames]:Received multicast frames
- [OversizeFrames]:Oversize frames
- [UndersizeFrames]:undersize frames
- [CrcError]:number of CRC error
- [SendBytes]:sending bytes
- [SendFrames]:sending frames
- [SendBroadcastFrames]:sending broadcast frames
- [SendMulticastFrames]:sending multicast frames

Configuration Information

Click directory tree **Monitoring > Running config** on the left of main page, open configuration information page, as shown in Figure 107. This page displays configuration information of switch.

FIGURE 107 CONFIGURATION INFORMATION PAGE



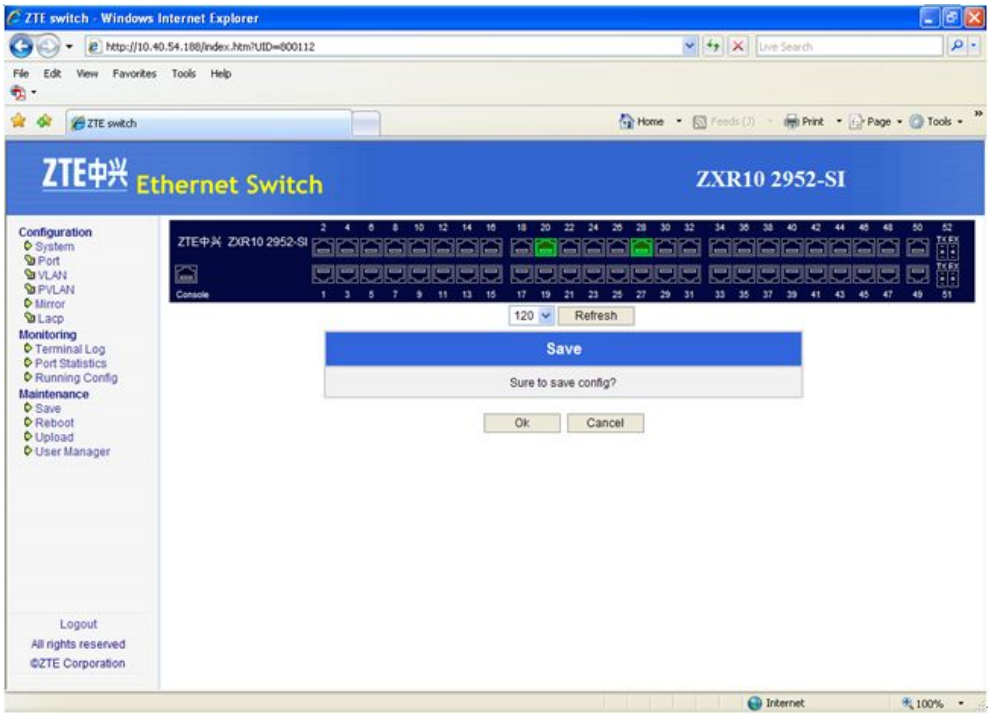
This page displays configuration information of switch.

System Maintenance

Saving Configuration

Click directory tree **Maintenance > Save** on the left of main page, open saving configuration information page, as shown in Figure 108.

FIGURE 108 SAVING CONFIGURATION PAGE



Click **Ok** to save configuration or click **Cancel** to cancel configuration.

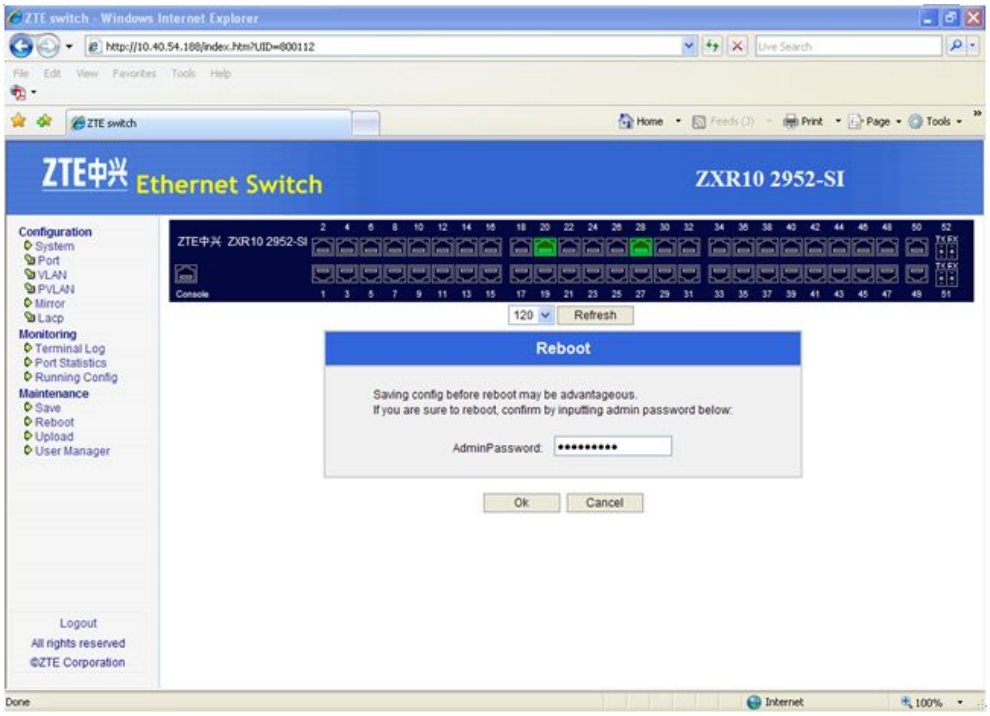
Caution:

Saving configuration will cover the original configuration file. Make sure that the configuration need to be covered before clicking **Ok**.

Configuring Reboot

Click directory tree **Maintenance > Reboot** on the left of main page, open reboot function page, as shown in Figure 109.

FIGURE 109 REBOOT FUNCTION PAGE

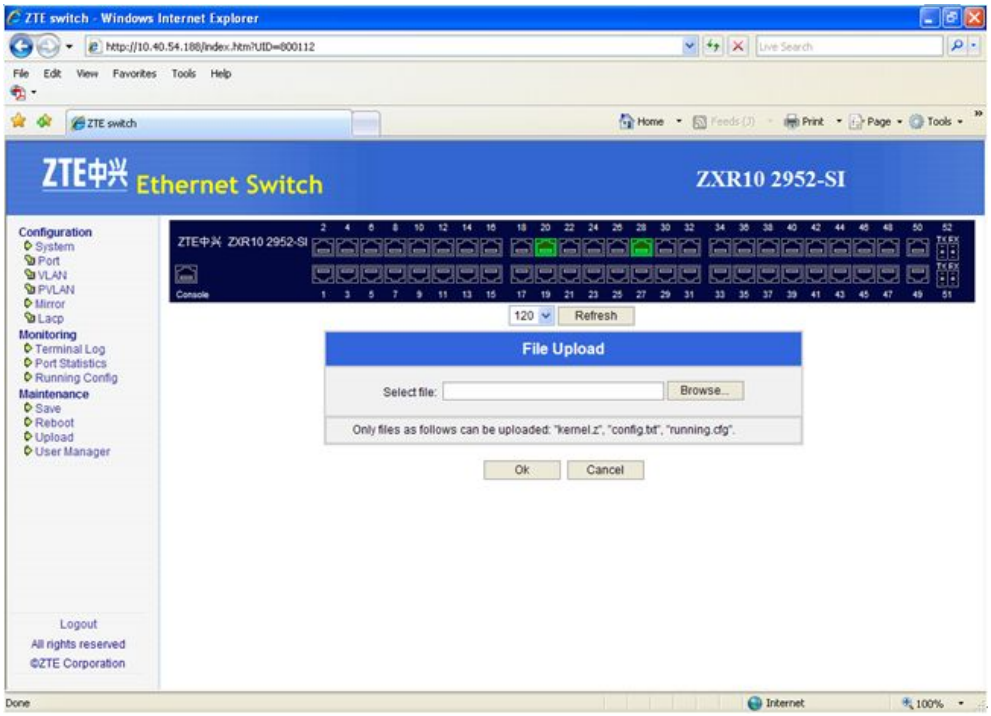


Enter Admin password in AdminPassword and then click **Ok** to reboot the switch or click **Cancel** to cancel reboot.

Uploading File

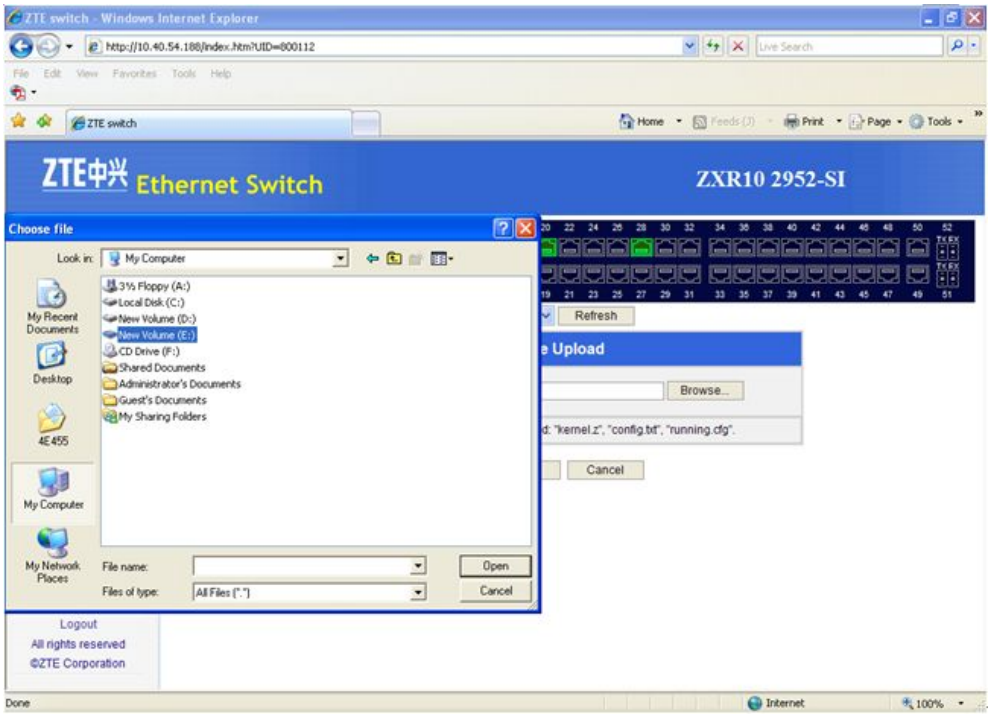
Click directory tree **Maintenance > Upload** on the left of main page, open file upload page, as shown in Figure 110.

FIGURE 110 FILE UPLOAD PAGE



Click **Browse...**, browse and select the file to be uploaded, as shown in Figure 111, and then click **Ok** to upload file.

FIGURE 111 BROWSE AND SELECT THE FILE



Note:

For safety and application, only allow "running.cfg","config.txt" and "kernel.z" to be uploaded.

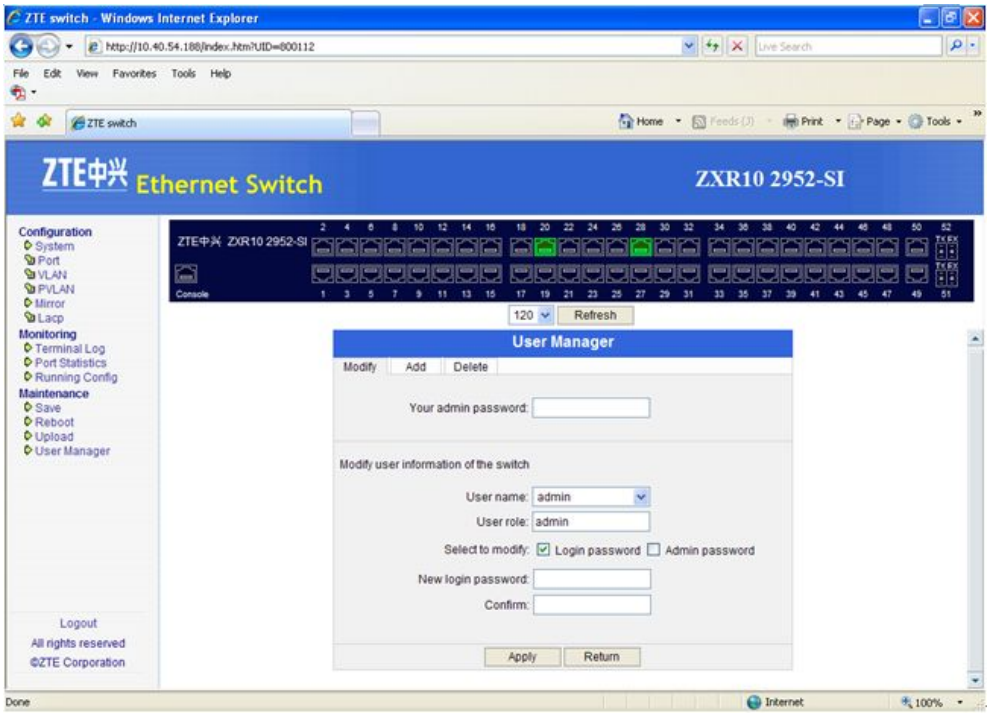
Caution:

Make sure the legality and validity of file to be uploaded. The uploaded file will cover the original file. If the operation is not correct switch can't work. Unprofessional personnel are not recommended to use this function.

User Management

Click directory tree **Maintenance > User Manager** on the left of main page, open user management page, as shown in Figure 112.

FIGURE 112 USER MANAGEMENT PAGE

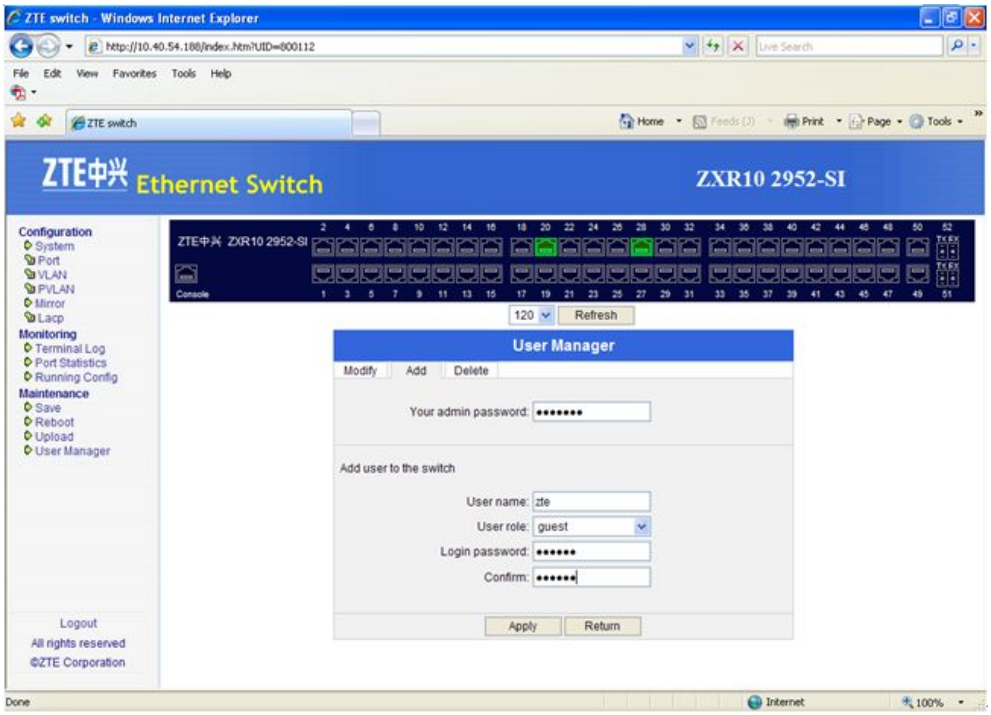


This page displays the current username. The username and login password can be modified. Enter the new username, password and new password and verify. Click **Apply** to submit.

Adding User

Click **add** button in user management page, open Adding User page, as shown in Figure 113

FIGURE 113 ADDING USER PAGE

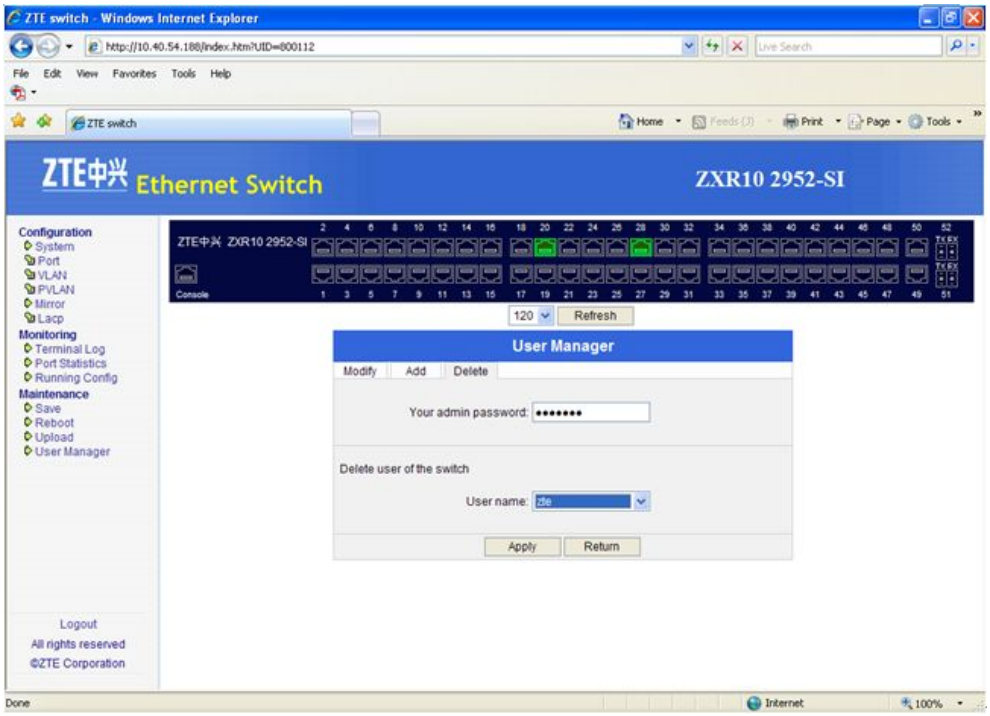


Enter admin password of current user in this page, enter the information about the user to be added, and then click **Apply** to submit.

Deleting User

Click **Delete** button in user management page, open Deleting User page, as shown in Figure 114.

FIGURE 114 DELETING USER PAGE



Enter admin password in this page, select the user to be deleted, and then click **Apply** to submit.

This page is intentionally blank.

Figures

Figure 1 ZXR10 2920/2928/2952/2936-FI Working Principle....12
Figure 2 ZXR10 2920 Front Panel....12
Figure 3 Front Panel Of ZXR10 2928 14
Figure 4 ZXR10 2952 Front Panel....15
Figure 5 ZXR10 2936-FI Front Panel....17
Figure 6 RS-2800-2GE-RJ45 Sub-board(FGEI) 19
Figure 7 RS-2800-2GE-SFP Sub-board(FGFI)....20
Figure 8 RS-2800-2GE-SFPRJ45 Sub-board(FGFE) 20
Figure 9 RS-2800-2FE-SFP(FBFE) 21
Figure 10 RS-2800-1GE-SFF 21
Figure 11 ZXR10 2920/2928/2952/2936-FI Back Panel (DC power) 22
Figure 12 ZXR10 2920/2928/2952/2936-FI Back Panel (AC power) 22
Figure 13 Installing Plastic Pads....23
Figure 14 Installing Flanges 24
Figure 15 Installing Brackets 24
Figure 16 Fixing the Switch 25
Figure 17 AC Power Cable 25
Figure 18 Outline Drawing of -48V Power Socket....26
Figure 19 DC Power Cable....26
Figure 20 Grounding Protect Cable 27
Figure 21 SERIAL PORT CONFIGURATION CABLE 27
Figure 22 STRUCTURE OF NETWORK CABLE 28
Figure 23 TRANSVERSE ENGLISH LABEL ON PANELS AND CONNECTORS 30
Figure 24 ROLL-TYPE SELF-COVER LASER PRINT LABEL MODEL II 31
Figure 25 TRANSVERSE ENGLISH TYPE I LABEL 31
Figure 26 PATTERN AND MEANINGS OF THE ENGINEERING LABEL ON THE OPTICAL FIBER 32
Figure 27 CABLING OF THE ETHERNET SWITCH IN A BUILDING....33
Figure 28 CABLING OF A CONVERGENCE SWITCH 34

Figure 29 STARTING THE HYPERTERMINAL.....35
Figure 30 LOCATION INFORMATION 35
Figure 31 SETTING UP A CONNECTION.....36
Figure 32 CONNECTION CONFIGURATION.....37
Figure 33 COM1 PROPERTIES.....38
Figure 34 ZXR10 2920/2928/2952/2936-FI CONFIGURATION MODES 43
Figure 35 RUNNING THE TELNET 45
Figure 36 SWITCH REMOTE LOGIN WINDOW.....45
Figure 37 TFTPD INTERFACE 58
Figure 38 TFTPD SETTINGS DIALOG BOX.....58
Figure 39 FDB Configuration Example.....72
Figure 40 Port Mirroring Configuration Example 74
Figure 41 EXAMPLE OF VLAN TRANSPARENT TRANSMISSION...81
Figure 42 GVRP Configuration Example.....82
Figure 43 PVLAN CONFIGURATION EXAMPLE 1 85
Figure 44 PVLAN CONFIGURATION EXAMPLE 2 85
Figure 45 TYPICAL QINQ NETWORKING.....86
Figure 46 QinQ Configuration Example 88
Figure 47 SQinQ Typical Network.....91
Figure 48 EXAMPLE OF LACP CONFIGURATION 93
Figure 49 MSTP Topological Structure.....95
Figure 50 STP Configuration Example.....99
Figure 51 ZESR running state when the ring is “complete state” 104
Figure 52 ZESR running state when the ring is “link failure” ..105
Figure 53 ZESR running state when the ring is “link restore” ..105
Figure 54 Multi-Ring Multi-Domain 106
Figure 55 ZESR Multi-Ring Multi-Domain Design Figure.....106
Figure 56 Non level 0 Segment Link 107
Figure 57 SMART-LINK 107
Figure 58 Tangent Ring Design Figure.....108
Figure 59 ZESR Single Ring Networking 112
Figure 60 ZESR multi ring networking 114
Figure 61 smart link networking 117
Figure 62 NETWORK TOPOLOGY FOR ONE-TO-MANY COMMUNICATION 123
Figure 63 IPTV Configuration Example.....129
Figure 64 DHCP CLIENT Configuration Example 133
Figure 65 DHCP Snooping Configuration Example.....136

Figure 66 Typical Network Of Vbas 137
Figure 67 EPON Configuration Example..... 144
Figure 68 ACL Configuration Example 155
Figure 69 QoS Configuration Example..... 165
Figure 70 l2pt Configuration Example 168
Figure 71 Layer-3 Configuration Example..... 171
Figure 72 USING PAP MODE FOR IDENTITY AUTHENTICATION..... 173
Figure 73 USING CHAP MODE FOR IDENTITY AUTHENTICATION..... 174
Figure 74 USING EAP MODE FOR IDENTITY AUTHENTICATION..... 175
Figure 75 Access Authentication Configuration Example 181
Figure 76 Remote Loop Network 190
Figure 77 Link Control Network 191
Figure 78 SSH CONFIGURATION EXAMPLE 196
Figure 79 SETTING IP ADDRESS AND PORT NUMBER OF THE SSH SERVER..... 197
Figure 80 SETTING SSH VERSION NUMBER..... 197
Figure 81 USER CONFIRMATION REQUIRED IN THE FIRST LOGIN..... 198
Figure 82 SSH LOGIN RESULT 198
Figure 83 CLUSTER MANAGEMENT NETWORKING..... 206
Figure 84 SWITCH ROLE CHANGEOVER RULE 207
Figure 85 System Login Interface 215
Figure 86 System Main Interface 216
Figure 87 System Information Page 217
Figure 88 Port State Information Page 218
Figure 89 Port Configuration Information Page..... 219
Figure 90 Single Port Configuration Page 220
Figure 91 Bulk Port Configuration Page 221
Figure 92 VLAN Information Page 222
Figure 93 VLAN Number Entering Page 223
Figure 94 Single VLAN Configuration Page..... 223
Figure 95 Bulk VLAN Configuration Page 224
Figure 96 PVLAN Information Page..... 225
Figure 97 PVLAN Configuration Page 226
Figure 98 Mirror Information Page 227
Figure 99 Port Ingress Mirroring Configuration Page 228
Figure 100 Port Egress Mirroring Configuration Page..... 228

Figure 101 LACP Basic Attribute Page 229
Figure 102 Bulk Aggregation Port Configuration Page..... 230
Figure 103 Aggregation Group Information Page 231
Figure 104 Aggregation Group Configuration Page..... 232
Figure 105 Terminal Log Information Page 233
Figure 106 Port Statistics Information Page 234
Figure 107 Configuration Information Page 235
Figure 108 Saving Configuration Page 236
Figure 109 Reboot Function Page 237
Figure 110 File Upload Page 238
Figure 111 Browse and Select the File 238
Figure 112 User Management Page 239
Figure 113 Adding User Page 240
Figure 114 Deleting User Page..... 241

Tables

Table 1 Technical Features and Parameters..... 8
Table 2 Indicator Working State of ZXR10 2920 13
Table 3 Indicator Working State of ZXR10 2928 15
Table 4 Indicator Working State of ZXR10 2952 16
Table 5 Indicator Working State of ZXR10 2936-FI 18
Table 6 ZXR10 2920/2928 Sub-board List 18
Table 7 PINOUT OF SERIAL PORT CONFIGURATION CABLE 27
Table 8 RJ45 PINOUT OF STRAIGHT-THROUGH CABLE 28
Table 9 RJ45J PINOUT OF CROSSOVER CABLE 29
Table 10 FIBER TYPES 29
Table 11 TEMPERATURE AND HUMIDITY TABLE 39
Table 12 FUNCTIONAL KEYS.....53
Table 13 Port Role and Port State.....96
Table 14 Syslog Log Information..... 182

This page is intentionally blank.

Glossary

ACL
- Access Control List

ARP
- Address Resolution Protocol

DHCP
- Dynamic Host Configuration Protocol

IGMP
- Internet Group Management Protocol

IP
- Internet Protocol

LACP
- Link Aggregation Control Protocol

MAC
- Medium Access Control

MSTP
- Multiple Spanning Tree Protocol

NTP
- Network Time Protocol

OAM
- Operation, Administration and Maintenance

PVID
- Port VLAN ID

PVLAN
- Private Virtual Local Area Network

RMON
- Remote Monitoring

RSTP
- Rapid Spanning Tree Protocol

SNMP
- Simple Network Management Protocol

SP
- Strict Priority

SSH
- Secure Shell

STP
- Spanning Tree Protocol

TFTP
- Trivial File Transfer Protocol

VBAS
- Virtual Broadband Access Server

VLAN
- Virtual Local Area Network

WRR
- Weighted Round Robin

ZESR
- ZTE Ethernet Switch Ring